

Sociální inženýrství jako hrozba pro starší generace: prevence a osvěta

Maksym Nebytov

Bakalářská práce
2025



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav bezpečnostního inženýrství

Akademický rok: 2024/2025

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	Maksym Nebytov
Osobní číslo:	A22239
Studijní program:	B1032A020001 Bezpečnostní technologie, systémy a management
Forma studia:	Prezenční
Téma práce:	Sociální inženýrství jako hrozba pro starší generace: prevence a osvěta

Zásady pro vypracování

- Zpracujte literární rešerši na dané téma.
- Popište základní techniky sociálního inženýrství a jejich specifické využití pro starší populaci.
- Zaměřte se na analýzu důvodů, proč jsou lidé starší populace častějšími oběťmi těchto útoků.
- Navrhněte preventivní nástroje a postupy, které mohou starší generaci lépe ochránit, s důrazem na osvětu a vzdělávání.

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. Jirásek, Petr, Luděk Novák a Josef Požár. Výkladový slovník kybernetické bezpečnosti: Cyber security glossary. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.
2. Benzl, Lukáš. 2024. Deepfake 2024: Obranná strategie pro české firmy. Praha: Česká asociace umělé inteligence. Dostupné z: <https://asociace.ai>
3. Engebretson, Patrik. 2011. The Basic of Hacking and Penetration Testing. Ethical Hacking and Penetration Testing Made Easy. Waltham: Elsevier.
4. Bešić, Mustafa. 2023. Benefits and Risks of Artificial Intelligence in Cybersecurity and Phishing Attacks. Master of Social Informatics. International Business and Information Academy, Tuzla, Bosnia and Herzegovina.
5. Štěpánek, Zdeněk. 2020. Inženýrství sociální. Sociologická encyklopedie. Praha: Sociologický ústav AV ČR.

Vedoucí bakalářské práce: **Ing. Petra Dostálová**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **11. prosince 2024**

Termín odevzdání bakalářské práce: **2. června 2025**

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan



Ing. Jan Valouch, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 11. prosince 2024

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že

- odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení bakalářské práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 mohu užít své dílo – bakalářskou práci – nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá; neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji, že

- jsem na bakalářské práci pracoval(a) samostatně a použitou literaturu jsem řádně citoval(a); v případě publikace výsledků budu uveden(a) jako spoluautor;
- odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

Ve Zlíně, dne

.....
podpis autora

ABSTRAKT

Bakalářská práce se zaměřuje na fenomén sociálního inženýrství, přičemž klíčovým tématem je zranitelnost starší populace vůči podvodným a manipulativním technikám. Sociální inženýrství zahrnuje metody, které útočníci využívají k neoprávněnému získání důvěrných informací nebo přístupu k zabezpečeným systémům. Cílem práce je analyzovat strategie, kterými podvodníci oslovují a klamou seniory. Výzkum se zabývá různými formami útoků, jako jsou phishing, vishing a smishing, a klade důraz na prevenci rizik. V praktické části jsou zkoumány konkrétní případy podvodů zaměřených na starší osoby, provádí se dotazníkové šetření a navrhuje se konkrétní opatření ke zvýšení ochrany seniorů. Výstupem práce je posílení povědomí o těchto hrozbách a návrh efektivních preventivních strategií.

Klíčová slova: sociální inženýrství, senioři, kybernetická bezpečnost, dotazníkové šetření

ABSTRACT

The bachelor's thesis focuses on the phenomenon of social engineering, with a key theme being the vulnerability of the elderly population to fraudulent and manipulative techniques. Social engineering involves methods that attackers use to gain unauthorized access to confidential information or secure systems. The objective of this paper is to analyze the strategies that fraudsters use to reach and deceive the elderly population. The research examines various forms of attacks such as phishing, vishing and smishing, and emphasizes risk prevention. In the practical part, specific cases of scams targeting the elderly are examined, a questionnaire survey is conducted, and specific measures are proposed to increase the protection of seniors. The outcome of the work is to increase awareness of these threats and to propose effective prevention strategies.

Keywords: social engineering, older people, cybersecurity, questionnaires

Chtěl bych srdečně poděkovat vedoucí mé Bakalářské práce paní inženýrce Petře Dostálové za její ochotu, vstřícnost a cenné rady, které mi během psaní této bakalářské práce velmi pomohly.

Mé upřímné poděkování patří také mé rodině a přátelům za jejich neustálou podporu a motivaci po celou dobu mého studia.

Velké díky patří všem respondentům, kteří se zúčastnili dotazníkového šetření, a všem, kdo mi pomohli s jeho šířením a zprostředkováním. Vaše ochota a spolupráce byly pro tuto práci nepostradatelné.

OBSAH

ÚVOD.....	11
I TEORETICKÁ ČÁST	12
1 VYMEZENÍ KLÍČOVÝCH POJMŮ	13
1.1 KYBERPROSTOR	13
1.2 KYBERNETICKÁ KRIMINALITA.....	13
1.3 KYBERNETICKÝ ÚTOK	14
1.4 SOCIOTECHNIKA.....	15
2 SOCIÁLNÍ INŽENÝRSTVÍ	16
2.1 PSYCHOLOGICKÉ PRINCIPY SOCIÁLNÍHO INŽENÝRSTVÍ	18
2.2 TYPOLOGIE OBĚTÍ SOCIÁLNÍHO INŽENÝRSTVÍ.....	19
2.2.1 Starší lidé.....	20
2.2.2 Zaměstnanci s nedostatečným školením	20
2.2.3 Lidé s nízkou úrovní digitální gramotnosti	21
2.3 TECHNOLOGICKÉ NÁSTROJE POUŽÍVANÉ V SOCIÁLNÍM INŽENÝRSTVÍ	22
2.3.1 Deepfake technologie.....	22
2.3.2 Chatboty a automatizované systémy	23
2.3.3 Malware.....	23
2.3.4 Sociální média a sledovací software	24
2.3.5 Phishingové nástroje s umělou inteligencí.....	24
2.4 PRÁVNÍ RÁMEC OCHRANY OSOBNÍCH ÚDAJŮ	25
3 TECHNIKY SOCIÁLNÍHO INŽENÝRSTVÍ	26
3.1 PHISHING.....	27
3.1.1 Mechanismus phishingových útoků	27
3.1.2 Formy phishingu	28
3.2 PRETEXTING	29
3.2.1 Princip a účinnost pretextingu	29
3.3 BAITING	29
3.4 VISHING	30
3.5 SMISHING	30
4 STARŠÍ GENERACE.....	32
4.1 SENIOŘI A INFORMAČNÍ TECHNOLOGIE	33
4.2 AKTIVITY STARŠÍ GENERACE V KYBERPROSTORU	34
4.3 SENIOŘI JAKO SNADNÝ CÍL SOCIÁLNÍHO INŽENÝRSTVÍ	34
4.4 ZRANITELNOST STARŠÍ GENERACE VŮČI KYBERNETICKÝM PODVODŮM A STRATEGIE PREVENCE	35
II PRAKTICKÁ ČÁST.....	38

5	ANALÝZA KONKRÉTNÍCH PODVODŮ ZAMĚŘENÝCH NA SENIORY	39
5.1	INZERÁT NA INTERNETU	39
5.2	PŘÍPAD VISHINGU Z DĚČÍNSKA	40
5.3	PŘÍPAD VISHINGU Z TÁBORSKA	41
5.4	PŘÍPAD PODVODU PŘI INVESTOVÁNÍ	42
6	POVĚDOMÍ O SOCIÁLNÍM INŽENÝRSTVÍ U STARŠÍ GENERACE	45
6.1	CÍL ŠETŘENÍ.....	45
6.2	ZPRACOVÁNÍ ŠETŘENÍ	45
6.3	CÍLOVÁ SKUPINA A VÝBĚR ÚČASTNÍKŮ	46
6.4	ZKOUMANÉ VÝSLEDKY DOTAZNÍKU	49
6.5	VÝSLEDKY ŠETŘENÍ.....	58
6.5.1	Vyhodnocení hypotézy	58
7	NÁVRH PREVENTIVNÍCH NÁSTROJŮ A POSTUPŮ PRO OCHRANU STARŠÍ GENERACE	60
7.1	PRÁVIDELNÉ VZDĚLÁVACÍ SEMINÁŘE A ŠKOLENÍ	60
7.2	EDUKAČNÍ MATERIÁLY A KAMPANĚ	60
7.3	RODINNÁ OSVĚTA.....	61
7.4	INFORMOVÁNÍ SKRZE MÉDIA	61
7.5	TECHNICKÁ OPATŘENÍ.....	61
	ZÁVĚR.....	63
	SEZNAM POUŽITÉ LITERATURY	65
	SEZNAM OBRÁZKŮ	71
	SEZNAM GRAFŮ	72
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	73
	SEZNAM PŘÍLOH.....	74

ÚVOD

S dynamickým rozvojem digitálních technologií a postupnou implementací internetu do všech oblastí každodenního života dochází nejen ke zkvalitňování služeb, ale současně i k nárůstu počtu a sofistikovanosti kybernetických hrozeb. Jednou z nejzávažnějších, a zároveň nejhůře identifikovatelných metod útoku, je právě sociální inženýrství. Jedná se o manipulativní techniku, jež necílí na technické slabiny, ale na nejzranitelnější součást bezpečnostního řetězce, kterým je člověk. Útočník využívá sociální inženýrství k tomu, aby oběť přiměl k dobrovolnému poskytnutí citlivých informací či k vykonání určitých kroků, aniž by si oběť uvědomovala jejich skutečný význam.

Starší generace představují z hlediska zranitelnosti vůči sociotechnickým útokům vysoce rizikovou skupinu. Tito lidé se v běžném životě čím dál častěji dostávají do kontaktu s digitálním prostředím, ovšem bez dostatečné průpravy a bezpečnostní gramotnosti. Mnozí z nich nemají dostatečné povědomí o možných rizicích a vyznačují se zvýšenou důvěřivostí vůči neautentickým zprávám či podvrženým webovým stránkám. Na rozdíl od mladší generace, která je s technologiemi více sžitá, senioři často postrádají dovednosti a znalosti, které by jim umožnily těmto útokům účinně čelit. Právě proto jsou útočníky vnímáni jako snadný cíl.

Sociální inženýrství tak nelze chápat pouze jako technický problém či psychologický jev, ale především jako závažnou společenskou výzvu, která se týká značné části populace. Klíčovým nástrojem obrany je prevence a cílená osvěta.

Cílem této bakalářské práce je zhodnotit informovanost seniorů o útocích založených na principech sociálního inženýrství. Dotazníkové šetření se zaměřuje na to, zda respondenti zažili podvody typu phishing, smishing nebo vishing, a zároveň zkoumá jejich slabiny vůči těmto útokům a dosavadní zkušenosti. Práce analyzuje tyto slabiny v teoretické části, která přináší přehled klíčových pojmů a metod sociálního inženýrství, a v praktické části vycházející z reálných dat.

Na základě výsledků výzkumu jsou navržena konkrétní opatření, jejichž cílem je zvýšení povědomí seniorů o sociotechnických hrozbách a posílení jejich schopnosti těmto útokům odolávat a správně reagovat.

Osobní motivací pro výběr tohoto tématu je dlouhodobý zájem o problematiku lidského faktoru v oblasti kybernetické bezpečnosti a dále pak inspirace odbornou literaturou.

I TEORETICKÁ ČÁST

1 VYMEZENÍ KLÍČOVÝCH POJMŮ

Pro pochopení principů sociálního inženýrství je nezbytné vymezit několik základních pojmů, které tvoří rámec celé problematiky. Následující podkapitoly se zaměřují na vymezení klíčových pojmů, jako jsou kyberprostor, kybernetická kriminalita, kybernetický útok a sociotechnika.

1.1 Kyberprostor

V současné době informačních technologií, které hrají klíčovou roli v chodu firem i celé společnosti, se stává kyberprostor nezbytným pojmem pro pochopení moderního online prostředí a souvisejících bezpečnostních rizik.

Kyberprostor představuje digitální prostředí, v němž dochází ke vzniku, zpracování a sdílení informací, které je tvořeno informačními systémy, elektronickými komunikačními sítěmi a souvisejícími službami. Český kyberprostor je pak specifický kyberprostor, který spadá pod jurisdikci České republiky. [1] [2]

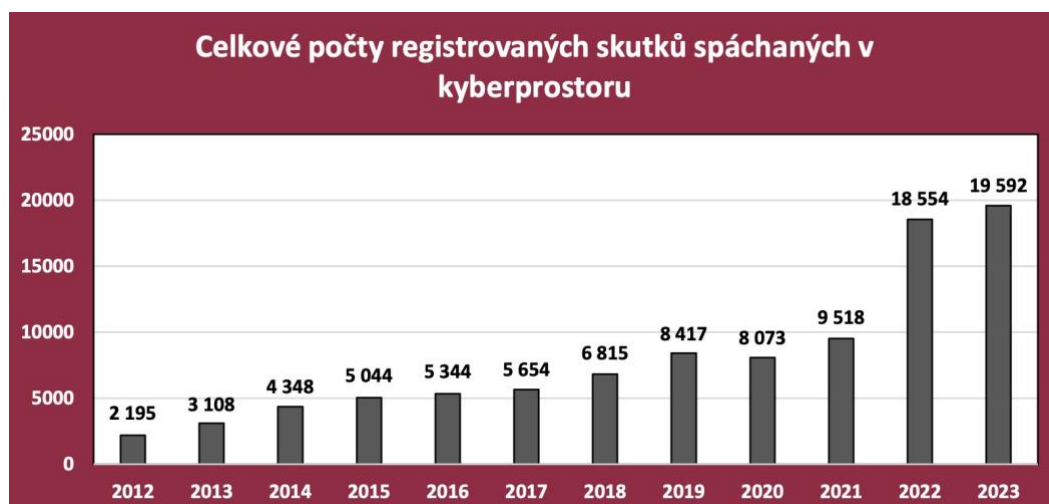
V tomto prostředí se odehrává široká škála aktivit, od běžné komunikace a přístupu k informacím, přes obchodní transakce a správu státních záležitostí, až po provoz kritické infrastruktury. S rostoucí závislostí na informačních systémech a elektronických komunikacích se kyberprostor stává zásadním prostředím pro fungování moderní společnosti.

Nicméně, toto digitální prostředí je také dějištěm různých útoků, souhrnně označovaných jako kybernetické útoky. Pojem kyberprostor je tedy klíčový pro pochopení nejen technologického vývoje, ale i bezpečnostních výzev, kterým moderní společnost čelí. Jeho zabezpečení a ochrana jsou zásadní pro zachování funkčnosti státu, ekonomiky, bezpečnosti občanů a firem. V tomto digitálním prostoru se také vyskytují hrozby, které využívají lidskou psychologii prostřednictvím metod sociálního inženýrství. [1] [2] [3]

1.2 Kybernetická kriminalita

Kybernetická kriminalita představuje trestnou činnost, při níž hraje roli počítač, a to jako celek zahrnující technické i softwarové vybavení včetně dat, jeho jednotlivé části, nebo větší počet počítačů, které fungují samostatně nebo jsou vzájemně propojeny do sítě. Tyto prvky mohou být buď samotným cílem útoku, nebo mohou sloužit jako prostředí či nástroj pro spáchání dané trestné činnosti. [2]

Mezi lety 2011 a 2023 kybernetická kriminalita v České republice trvale rostla, s prudkým nárůstem v roce 2022, kdy překročila hranici 10 % z celkové kriminality. Rok 2023 přinesl mírnější 6% nárůst, k němuž přispěla i reakce státních a soukromých institucí. Přesto zůstává trend nadále vzestupný. Pachatelé své metody zdokonalují a stále častěji využívají nástroje umělé inteligence. [4] [5]



Graf 1 Celkové počty registrovaných skutků spáchaných v kyberprostoru

(zdroj: FOLDYNA, Tomáš. *Zpráva o činnosti národního zpravodaje pro boj proti kybernetické kriminalitě, pro ochranu práv k nehmotným statkům a kybernetickou bezpečnost za rok 2023. 2024.*)

1.3 Kybernetický útok

Kybernetický útok se zaměřuje na destabilizaci IT systémů s cílem poškodit je a nelegálně získat citlivé nebo klíčové informace, které mají vysokou strategickou hodnotu. Tyto útoky mohou mít různé cíle a projevy, a mohou být motivovány politicky, ekonomicky či kriminálně.

Kybernetická špionáž představuje další významný bezpečnostní problém, spočívající v cíleném získávání citlivých dat od jednotlivců či organizací prostřednictvím informačních technologií. S tímto jevem se dá často setkat v souvislosti se snahou o dosažení vojenské, politické nebo ekonomické výhody. [2]

V reakci na tyto hrozby je nezbytná kybernetická obrana, která se zaměřuje na prevenci útoků a zároveň na omezení jejich negativních důsledků. Důležitá je také schopnost jednotlivců nebo organizací odolávat těmto hrozbám a včas reagovat. Efektivní kybernetická obrana vyžaduje komplexní přístup, zahrnující technická opatření, bezpečnostní politiku a vzdělávání uživatelů. [2] [3]

1.4 Sociotechnika

Termín sociální inženýrství bývá často zaměňován s pojmem sociotechnika. Tyto dva výrazy se často prolínají a jde o téměř totožné pojmy. Oba pojmy čerpají z vědeckých poznatků oborů, jako jsou filozofie, psychologie, sociologie a ekonomie. Existence sociálního inženýrství je však spojena až s 20. stoletím, tedy s obdobím po vzniku moderních informačních technologií. Již před vznikem tohoto moderního pojetí však lidé využívali psychologické metody za účelem manipulace a klamání ostatních, ať už šlo o podvodníky, špióny či jiné osoby usilující o získání výhod. Sociotechnika se výrazně opírá o komunikační dovednosti, které do jisté míry používá každý člověk ve svém běžném životě. [6]

Kevin Mitnick ve své knize Umění klamu vysvětluje, že sociotechnici často působí sympaticky, chovají se zdvořile a díky těmto vlastnostem si rychle získávají důvěru i oblibu. Ti, kteří zvládnou taktiky a metody tohoto oboru, pak dokážou získat přístup k nejruznějším informacím. V praxi, zejména v kontextu kybernetické bezpečnosti, se však pro popis technik manipulace a ovlivňování nejčastěji používá označení sociální inženýrství. [7]

2 SOCIÁLNÍ INŽENÝRSTVÍ

Sociální inženýrství je technika využívající psychologickou manipulaci k získání citlivých informací, které mohou být následně zneužity při kybernetických či jiných typech útoků. Útočník využívá různé formy klamu a přesvědčování, aby v oběti vyvolal důvěru a přiměl ji k určitému jednání. Obvyklým cílem útočníků jsou například hesla, údaje o platebních prostředcích nebo přímý přístup k zařízení. Účinnost této metody spočívá zejména v její nenáročnosti, místo technického prolomení zabezpečení postačí, když oběť své údaje poskytne sama. Lidský faktor je tedy klíčovou zranitelností, na kterou se útočníci zaměřují. Konečným cílem bývá získání neoprávněného přístupu nebo způsobení úniku dat. [2] [3] [8]

Sociologická encyklopedie definuje sociální inženýrství jako aplikovanou disciplínu v rámci praxeologie. Jejím cílem je na základě vědeckého poznání formulovat účinné praktické zásady a doporučení vedoucí ke společenským změnám nebo, v užším smyslu, ke změnám v chování a jednání jednotlivců či skupin. [6]

Jedná se o nejen velmi účinnou, ale zároveň pro zkušeného útočníka i relativně snadno proveditelnou metodu kompromitace i vysoce zabezpečených systémů. Útoky mají obvykle vysokou míru úspěšnosti a bývají obzvláště záluďné. Pokud útočník dokáže důkladně skrýt svou stopu, je jeho odhalení velice obtížné. [2] [3]

Oběti sociálního inženýrství si obvykle neuvědomují, že jsou cíleně ovlivňovány, což útočníkům usnadňuje získání citlivých informací. V době, kdy hrají informační technologie klíčovou roli v chodu firem i společnosti, se informace stávají nejen cenným aktivem, ale také častým cílem podvodných aktivit. Sociální inženýrství v oblasti informačních technologií lze definovat jako formu manipulace, která spoléhá na psychologické metody přesvědčování a zneužívání lidské důvěřivosti. [3] [7]

Často se předpokládá, že narušení bezpečnosti počítačových systémů je primárně důsledkem technických nedostatků a chyb v softwaru, které útočník dokáže využít. Ve skutečnosti však významnou roli sehrává právě sociální inženýrství, které umožňuje útočníkům obejít zabezpečení jednodušší cestou. Nízká úroveň povědomí uživatelů o hrozbách často otevírá dveře k jejich manipulaci, čímž se mohou stát neúmyslnými prostředníky umožňujícími neoprávněný přístup k systému. [3] [9]

Zneužívání lidského rozhodování, především prostřednictvím kognitivních chyb a zkreslení, je základní technikou v oblasti sociálního inženýrství. Útočník tak dokáže využít nejslabší složku bezpečnostního systému, kterou v tomto kontextu představuje člověk.

Zatímco software je navržen tak, aby vykonával přesně definované operace, lidské reakce vycházejí z individuálních zkušeností, smyslového vnímání a emocionálního stavu. Tento faktor činí člověka obzvláště citlivým na manipulativní techniky, které mohou útočníci využít k dosažení vlastních záměrů. [1] [9]

Někteří útočníci se zaměřují na budování mezilidských vztahů s oběťmi, cílem je navodit atmosféru důvěry. Riziko sociálního inženýrství spočívá v jeho nenápadnosti a snadném uplatnění. Lidé jsou dnes zvyklí na časté telefonáty, e-maily a každodenní komunikaci se známými i neznámými osobami. Každý den člověk odpovídá na desítky e-mailů a navštěvuje různé webové stránky. Jsme neustále vystaveni sociální interakci, zahrnující nejrůznější požadavky, konverzace, otázky a úkoly. Pro zkušeného útočníka není problém v této běžné rutině splynout s okolím. Sociální inženýři tak dokážou využít každodenní vzorce chování a nenápadně z oběti získat citlivé informace. Často se stává, že při zpětném šetření úniku citlivých dat si oběť neuvědomuje svou chybu, protože interakce s útočníkem jí připadala jako běžná součást pracovního či osobního života. V některých případech si dokonce není schopna vzpomenout, kdy a komu své údaje sdělila. [7] [10] [11]

Útočníci čerpají z obrovského množství informací dostupných na internetu. Tyto informace, zejména ze sociálních médií, umožňují detailní profilování obětí. Útočníci tak mohou snadno dohledat osobní údaje, pracovní zkušenosti a zájmy oběti. Tímto způsobem mohou útočníci lépe pochopit chování oběti a vytvořit zcela personalizovaný útok, například phishingovou kampaň. Dále mohou zneužít specifické technické nástroje a metody vyhledávání, včetně analýzy metadat. Celkově platí, že čím více informací útočníci mají, tím větší je pravděpodobnost úspěchu útoku. Z tohoto důvodu je potřeba, aby byl kladen důraz na opatrnost při sdílení osobních údajů online a na ochranu firemních informací. [10] [12]

Využití sociálního inženýrství není omezeno pouze na nezákonné aktivity, ale nachází své místo i v legálních oblastech. V nezákonných aktivitách se využívá k získání citlivých informací nebo k neoprávněnému přístupu k systémům, zatímco v legálních oblastech je naopak sociální inženýrství využíváno k testování bezpečnosti organizací (penetrační testování), vzdělávání o bezpečnostních hrozbách nebo v rámci spolupráce s orgány činnými v trestním řízení. Tento nástroj tedy může být použit jak pro dobré účely, jako je zlepšení bezpečnosti, tak pro účely nelegálního zneužívání. [1] [9]

Metody sociálního inženýrství se neustále vyvíjejí a přizpůsobují se novým podmínkám, což znamená, že je nutné, aby organizace i jednotlivci byli stále v pohotovosti. Útočníci neustále hledají nové způsoby, jak využít psychologické techniky k manipulaci

obětí, což zajišťuje, že metody, které byly účinné v minulosti, mohou dnes ztrácet na efektivitě. S rozvojem digitálních technologií, růstem vlivu sociálních médií a novými komunikačními kanály se útočníkům otevírá stále širší prostor pro vytváření nových a sofistikovanějších forem podvodů. Tento rychlý vývoj klade důraz na nutnost sledování nových trendů a technik v oblasti ochrany proti těmto hrozbám. [7] [10]

2.1 Psychologické principy sociálního inženýrství

Teoretickým základem sociálního inženýrství je analýza lidského chování a psychologie, jejímž cílem je manipulace jednotlivců k vykonání určitých činností nebo k poskytnutí informací. Na rozdíl od technických kybernetických útoků zaměřuje sociální inženýrství svou pozornost na člověka, který bývá považován za nejslabší složku bezpečnostních systémů. [13]

Útočníci v rámci sociálního inženýrství často zneužívají princip recipacity, tedy lidskou potřebu oplatit laskavost. I nenápadné věci, jako je pochvala, mohou navodit dojem určitého závazku. Tento princip funguje na základě podvědomé povinnosti oběti odvděčit se za přijatou pomoc, což nemusí mít nutně materiální podobu. Může jít například o poskytnutí informací nebo provedení určité akce. [10] [14]

Další psychologickou metodou je využití ústupku, kdy útočník nejprve předloží větší požadavek, který oběť odmítne, a následně předloží menší požadavek, u kterého mu oběť vyhoví. Útočníci mohou také vytvořit situaci, kdy se oběť cítí dlužná, což ji motivuje k poskytnutí informací nebo ke spolupráci. Tyto techniky často probíhají na úrovni automatických kognitivních reakcí, které si oběti ani neuvědomují. [7] [10]

V kontextu sociálního inženýrství se využívá i princip zneužívání autority, který je založen na přirozené tendenci lidí následovat pokyny těch, které vnímají jako autoritativní osoby. Tato tendence je hluboce zakotvena v lidském chování, kdy máme tendenci důvěřovat osobám, které vykazují známky autority. Může se jednat o vyšší postavení, odborné znalosti nebo důvěryhodnost. Útočníci, kteří tuto tendenci zneužívají, se často vydávají za osoby s reálnou nebo domnělou autoritou. Tímto způsobem se snaží přimět své oběti k tomu, aby vykonaly určité akce, které by za jiných okolností neprovedly. Tento manipulativní přístup je v sociálním inženýrství velmi efektivní, protože vyvolává dojem, že požadavky jsou legitimní a je nutné jim vyhovět. [12] [15]

Jedním z významných mechanismů využívaných v oblasti sociálního inženýrství je princip sociální adaptace. Ten spočívá v tendenci lidí napodobovat chování ostatních, zejména v situacích, kdy si nejsou jistí. V kombinaci s přirozenou potřebou lidské sympatie ovlivňuje tento mechanismus rozhodování a činí jednotlivce náchylnějšími k manipulaci. Úzce s tím souvisí jev sociálního důkazu, který popisuje tendenci vnímat určité chování či informace jako věrohodné, pokud je pozitivně přijímáno okolím. Útočníci této zranitelnosti zneužívají například tím, že se vydávají za důvěryhodné osoby spojené se známými institucemi, čímž zvyšují pravděpodobnost úspěchu svého podvodného jednání. [7] [13] [16]

Klíčem k efektivní manipulaci bývá schopnost navodit sympatii a důvěru, jež jsou zásadní pro praktické využití psychologických principů. Hadnagy zdůrazňuje čtyři klíčové faktory, které ovlivňují míru důvěry. Fyzická atraktivita je první z nich, neboť lidé mají tendenci upřednostňovat to, co je pro ně esteticky atraktivní, což platí jak pro vzhled osob, tak pro produkty. Dalším faktorem je známost – lidé důvěřují tomu, co je jim známé, a to jak v kontextu lidí, tak v souvislosti se službami či výrobky. Komplimenty a projevy úcty jsou dalšími nástroji, které sociotechnici využívají k posílení vztahů a udržení oběti v interakci. Posledním faktorem je první dojem, který si o druhých vytváříme již během několika sekund setkání, přičemž sociotechnici tuto informaci využívají k tomu, aby se prezentovali jako důvěryhodní a sympatičtí jednotlivci. [10] [12]

Sociální inženýrství tak není pouze technikou manipulace, ale komplexním psychologickým procesem, který kombinuje různé principy lidského chování. Porozumění těmto mechanismům je zásadní nejen pro obranu jednotlivců, ale také pro vzdělávací programy a tvorbu bezpečnostních opatření.

2.2 Typologie obětí sociálního inženýrství

Využití psychologických principů a lidských slabin tvoří základ sociálního inženýrství, přičemž obětí těchto manipulativních technik se může stát kdokoliv. Neznalost a nedostatečné povědomí o taktikách sociálních inženýrů činí jednotlivce zranitelnými, protože mnoho lidí si neuvědomuje, jak snadno mohou být oklamáni. Důvěřivost jako přirozená součást mezilidských vztahů, je útočníky využívána k tomu, aby získali citlivé informace nebo si vybudovali falešnou autoritu. Faktory jako stres, časový tlak a neustálé rozptylování moderními technologiemi oslabují schopnost kriticky vyhodnocovat situace a snižují ostražitost. Útočníci rovněž cíleně pracují s emocemi, jako jsou strach, zvědavost nebo pocit naléhavosti, které mohou oběť přimět k jednání, jež by za běžných okolností

zvažovala pečlivěji. Nedostatečná znalost bezpečnostních zásad a preventivních opatření pak vede k vyššímu riziku, že se lidé stanou obětí manipulace. Určité skupiny obyvatel jsou pak vůči těmto útokům obzvláště náchylné. [7] [10] [13]

2.2.1 Starší lidé

Existuje řada faktorů, které činí starší populaci náchylnější k manipulaci prostřednictvím technik sociálního inženýrství. Jedním z hlavních je vyšší míra důvěřivosti, která je u seniorů často přirozenější než u mladších lidí, což z nich činí snadnější cíl pro podvodníky. [17] [18]

Další významnou příčinou atraktivity starších lidí pro podvodníky je jejich omezené povědomí o moderních formách podvodů a kybernetických hrozbách, protože senioři nemají vždy dostatečné zkušenosti s digitálním prostředím a souvisejícími riziky. Stárnutí také přináší určité změny kognitivních funkcí, jako je zhoršující se paměť nebo snížená schopnost rychlé reakce, což vede k menší ostražitosti vůči manipulativním praktikám. [13] [17] [19]

Vedle biologických aspektů se na zranitelnosti podílí i společenské faktory – starší lidé jsou ochotnější podvolit se autoritativním osobám. Problém sociální izolace navíc způsobuje, že osamělí senioři jsou citlivější na projevy pozornosti ze strany neznámých osob a mohou jim proto více důvěřovat. Tyto faktory společně vytvářejí podmínky, v nichž jsou starší lidé častěji oběťmi sociálního inženýrství. [17]

Podvody cílené na starší populaci představují rostoucí problém, který souvisí s technologickým pokrokem i měnící se dynamikou mezilidských vztahů. Moderní způsoby komunikace a digitalizace přinášejí nejen nové možnosti, ale i rizika, která mohou být obtížně rozpoznatelná. Zároveň se objevují stále promyšlenější manipulativní strategie, jež zneužívají individuální společenské faktory. Ochrana této ohrožené skupiny proto vyžaduje nejen technologická opatření, ale také větší důraz na informovanost a prevenci. [18] [20] [21]

2.2.2 Zaměstnanci s nedostatečným školením

Zaměstnanci s nedostatečnou znalostí bezpečnostních opatření čelí různým hrozbám, které útočníci využívají pomocí technik sociálního inženýrství. Tyto hrozby mohou vést k vážnému ohrožení bezpečnosti, finančním ztrátám a úniku citlivých údajů podniku. Mezi hlavní typy hrozeb pro danou skupinu patří:

- Phishing

- Vishing
- Smishing
- Baiting
- Pretexting
- Pharming
- Deepfakes
- Vnitřní hrozby

Pravidelná školení zaměřená na kybernetickou bezpečnost jsou nezbytná pro zvýšení povědomí zaměstnanců o těchto hrozbách a pro jejich schopnost rozpoznávat a předcházet těmto útokům. [7] [20]

Určité pracovní pozice a každodenní úkoly mohou zvyšovat zranitelnost zaměstnanců při manipulaci s citlivými informacemi. Tyto pracovní pozice zahrnují častý kontakt s externími subjekty, přístup k důvěrným datům nebo rutinní činnosti, které mohou být cílem útoků sociálního inženýrství. Administrativní pracovníci, recepční, zákaznická podpora či účetní jsou obvykle vystaveni většímu riziku, protože často komunikují s neznámými osobami a mají přístup k citlivým údajům. Noví zaměstnanci mohou být také náchylnější k podvodným praktikám, pokud nejsou dostatečně obeznámeni s firemní bezpečnostní politikou. [7]

Mezi každodenní úkoly, které zvyšují zranitelnost, patří nepozornost při zpracování e-mailů a telefonátů, sdílení informací bez ověření legitimacy příjemce, používání nezabezpečených komunikačních kanálů, nebo klikání na neznámé odkazy a přílohy. Také připojování neznámých USB zařízení může vést k zavlečení malwaru. K minimalizaci těchto rizik je nezbytné zaměřit se na školení zaměstnanců v oblasti kybernetické bezpečnosti a implementovat bezpečné komunikační kanály, ověřování totožnosti a dvoufaktorovou autentizaci. [7] [13] [22]

2.2.3 Lidé s nízkou úrovní digitální gramotnosti

Osoby s nízkou úrovní digitální gramotností jsou velmi náchylné k útokům sociálního inženýrství, což je dáno jejich omezenou schopností rozpoznat rizika v online prostředí. Často nemají dostatečné povědomí o běžných hrozbách, jako je phishing nebo malware, a nemohou tak rozpoznat varovné signály útoků. Dále se snadněji nechávají ovlivnit útočníky,

kterí využívají emoční nátlak. Nedostatek zkušeností s technologiemi také znamená, že může nastat problém s nastavením bezpečnostních opatření, jako jsou silná hesla nebo dvoufaktorové ověřování. V neposlední řadě bývají tito lidé ochotní sdílet citlivé informace, což z nich dělá snadné cíle pro podvodníky. [7] [16]

2.3 Technologické nástroje používané v sociálním inženýrství

Moderní metody sociálního inženýrství jsou stále sofistikovanější, a to především díky využití pokročilých technologií. Klíčovou roli zde hraje AI (umělá inteligence) spolu se syntetickým obsahem, jako je deepfake, který umožňuje vytvářet realistické, avšak falešné digitální obsahy. Současně kyberprostor a mobilní technologie poskytují útočníkům širší spektrum možností pro manipulaci a realizaci jejich podvodných strategií. [10] [23] [24] Další podkapitoly budou věnovány popisu nejčastějších technologických nástrojů používaných v sociálním inženýrství.

2.3.1 Deepfake technologie

Daná technologie se v kontextu sociálního inženýrství stává stále větším bezpečnostním rizikem, neboť umožňuje vytvářet extrémně realistické falešné multimediální obsahy. Útočníci tuto technologii využívají k podvodům, jako je vydávání se za důvěryhodné nebo známé osoby, manipulace prostřednictvím online schůzek, šíření nepravdivých informací a provádění phishingových a vishingových útoků. Tato technologie se také stává nástrojem kyberšikany a vydírání, přičemž její dopad může být pro oběti devastující. [23] [24]

Ochrana proti těmto útokům spočívá v kombinaci vzdělávání a technologických opatření. Klíčové je zvyšování povědomí o deepfakes, školení zaměstnanců a veřejnosti v oblasti identifikace podvrženého obsahu a rozvoj kritického myšlení při práci s digitálními informacemi. Důležitou roli hraje také implementace firemních bezpečnostních zásad, používání moderních detekčních softwarových nástrojů a důsledné ověřování identity při klíčových rozhodnutích. Vzhledem k neustálému vývoji deepfake technologií je nezbytné průběžně adaptovat obranné mechanismy a posilovat digitální bezpečnost. [7] [24]



Obrázek 1 Ukázka Deepfake

(zdroj: BENZL, Lukáš. *Deepfake 2024: Obranná strategie pro české firmy*. Praha: Česká asociace umělé inteligence, 2023. Dostupné také z: <https://asociace.ai/wp-content/uploads/2023/12/DEEPFAKE-2024-CAUI.pdf>.)

2.3.2 Chatboty a automatizované systémy

Chatboty představují v oblasti sociálního inženýrství sofistikovaný nástroj, který umožňuje útočníkům efektivně manipulovat uživateli a získávat citlivé informace. Díky pokročilé umělé inteligenci dokážou vést přirozené rozhovory a působit důvěryhodně. Mohou se vydávat za zaměstnance firem, technickou podporu či jiné autority, čímž vytvářejí iluzi legitimní komunikace. Mezi běžné taktiky patří automatizovaný phishing, sběr osobních údajů nebo přesměrování obětí na falešné webové stránky. Chatboty rovněž dokážou simulovat hlasovou konverzaci a provádět podvody prostřednictvím vishingu. Ochrana spočívá v ověřování identity odesílatele, kritickém přístupu k podezřelým žádostem a omezení sdílení citlivých dat online. [7] [10] [23]

2.3.3 Malware

Termín malware označuje škodlivé programy, jejichž účelem je obvykle narušení bezpečnosti a ochrany zařízení uživatele. Podle antivirového programu Avast se malware definuje jako software, který má za cíl získat neautorizovaný přístup k zařízení a provádět činnosti, jež mohou ohrozit integritu a bezpečnost uživatelských dat. Malware může manipulovat s těmito daty nebo ovlivnit fungování zařízení. Důležité je také si uvědomit, že

malware nepostihuje pouze osobní počítače, ale i mobilní telefony, servery a zařízení v rámci chytré domácnosti. [25] [26]

Mezi běžné typy malwaru patří například spyware, phishing, počítačové viry, červy, trojské koně, ransomware a rootkity. [26]

Malware se šíří prostřednictvím e-mailů, stahování souborů a infikovaných USB disků. Infekce často nastává kvůli nepozornosti uživatelů při otevírání podezřelých příloh a odkazů. Sociální inženýrství pomáhá útočníkům přimět oběť k instalaci malwaru. Následky mohou zahrnovat krádež dat, finanční ztráty nebo zpomalení zařízení. Malware může být součástí phishingového nebo baitingového útoku. Prevence zahrnuje aktualizovaný antivirový software, firewall a uživatelskou opatrnost při stahování souborů a připojování externích zařízení. [9] [26]

2.3.4 Sociální média a sledovací software

Sociální inženýři mohou využívat nástroje pro analýzu informací na sociálních sítích, kde se nachází široká škála osobních údajů o uživatelských aktivitách, zájmech a pracovních vztazích. Tyto informace jsou cenné pro personalizaci útoků. Útočníci mohou přizpůsobit své techniky a zaměřit se na konkrétní slabiny oběti, dále mohou využívat digitální stopy oběti na sociálních sítích a dalších technologických zařízeních k získání citlivých informací. Dané údaje mohou být použity k pochopení chování oběti, načasování útoku v nejzranitelnějších chvílích a potvrzení věrohodnosti vytvořené identity. Shromažďování informací je klíčovým krokem v procesu sociálního inženýrství, protože čím více informací útočník o oběti má, tím efektivněji může přizpůsobit svůj útok. [10] [12] [27]

2.3.5 Phishingové nástroje s umělou inteligencí

Umělá inteligence se stává významným nástrojem pro realizaci personalizovaných phishingových útoků. Technologie, jako jsou generativní modely AI, umožňují útočníkům rychle a efektivně vytvářet různé varianty útoků, čímž zvyšují šanci na jejich úspěch. Nástroje strojového učení mohou analyzovat chování cílové osoby na internetu a využívat tyto údaje k personalizaci útoků. Umělá inteligence je novým fenoménem v oblasti sociálního inženýrství, který umožňuje útočníkům shromažďovat informace o svých cílech a vykonávat efektivnější, personalizované útoky. [10] [23] [28]

2.4 Právní rámec ochrany osobních údajů

Jedním z hlavních cílů sociálních inženýrů je získání osobních údajů, může se jednat o jméno, rodné číslo, údaje o rodině, zvyklosti, kontakty nebo finanční situaci. Citlivé údaje pak zahrnují informace, které se týkají národnostního, etnického nebo rasového původu, politických názorů, členství v odborech, filozofického či náboženského přesvědčení, trestních odsouzení, zdravotního stavu, sexuální orientace a života subjektu údajů. Za citlivý údaj se rovněž považuje biometrický údaj a genetická informace, pokud umožňuje přímou identifikaci nebo ověření totožnosti dané osoby. Tyto informace slouží k vytvoření cíleného útoku. Útočník na základě informací vymyslí důvěryhodný příběh, který využívá získané osobní nebo citlivé údaje k manipulaci oběti a zvýšení šance na úspěšné oklamání. [29]

Právní ochrana těchto údajů má v ČR určitou tradici, dříve ji zajišťoval zákon č. 101/2000 Sb., o ochraně osobních údajů, který kladl důraz na povinnost organizací chránit data fyzických osob před zneužitím, neoprávněným zpřístupněním nebo únikem dat. [29]

V roce 2018 však ve všech členských státech EU vstoupilo v platnost Obecné nařízení o ochraně osobních údajů (GDPR, Nařízení EU 2016/679), které nahradilo dosavadní národní zákony včetně zákona č. 101/2000 Sb. a stanovilo jednotný rámec pro ochranu osobních údajů. GDPR posílilo práva jednotlivců zejména v oblasti informovanosti, souhlasu a přístupu k údajům. [30]

Nařízení GDPR dále definuje soubor zásad, kterými se musí správci a zpracovatelé řídit, zejména zákonnost, spravedlnost, transparentnost, omezení účelu, minimalizaci údajů, přesnost a omezení doby uchovávání. Klíčovým prvkem je princip odpovědnosti, jenž ukládá správcům povinnost zavést vhodná technická a organizační opatření k ochraně osobních údajů, čímž se minimalizuje riziko jejich zneužití. [30]

Právní ochrana je tedy nejen formální povinností organizací, ale i praktickým nástrojem obrany proti sociotechnickým útokům.

3 TECHNIKY SOCIÁLNÍHO INŽENÝRSTVÍ

Techniky sociálního inženýrství cílí především na lidskou chybu, důvěřivost a nedostatek znalostí o bezpečnostních rizicích. Na rozdíl od tradičních hackerských útoků, které cílí na technické zranitelnosti, se sociální inženýrství zaměřuje na nejslabší článek každého bezpečnostního systému – samotného uživatele. [27]

V průběhu let se sociální inženýrství vyvinulo v komplexní disciplínu, která kombinuje psychologické taktiky s moderními technologiemi. Útočníci mohou například využívat automatizované nástroje, umělou inteligenci nebo sofistikované digitální podvody k tomu, aby vytvořili důvěryhodné a přesvědčivé scénáře. Tyto metody jsou zaměřené jak na jednotlivce, tak na celé organizace, a díky své flexibilitě mohou být přizpůsobeny konkrétním situacím nebo obětí. [10] [11]

Jak již bylo uvedeno v minulých kapitolách, cílem útoků sociálního inženýrství je často získání přístupových údajů, finančních informací nebo jiných citlivých dat, která mohou být dále zneužita. Útočníci se při svých taktikách spoléhají na různé emocionální reakce, jako je důvěra, strach, zvědavost nebo pocit naléhavosti. Tyto reakce jsou stimulovány tak, aby oběť jednala impulzivně a bez uvažování. [10] [31]

Techniky sociálního inženýrství mohou být prováděny různými způsoby a prostřednictvím různých kanálů, od e-mailů, telefonních hovorů a textových zpráv až po osobní kontakt či využití sociálních sítí. Útočníci často vytvářejí situace, které působí legitimně a důvěryhodně, čímž snižují obezřetnost oběti. Falešná komunikace od důvěryhodné instituce nebo naléhavé zprávy, které vyžadují okamžitou akci, jsou běžnými příklady těchto praktik. [10] [11] [27]

Důvod, proč je sociální inženýrství tak účinné, spočívá ve schopnosti útočníků přizpůsobit své metody konkrétnímu cíli. Různé techniky mohou být použity k manipulaci jednotlivců na základě jejich role, technických znalostí, osobních zvyklostí nebo emocionálního stavu. To jim umožňuje dosahovat vysoké míry úspěšnosti. [10]

V následujících kapitolách budou podrobně rozebrány jednotlivé metody sociálního inženýrství, včetně jejich principů. Sociální inženýrství představuje hrozbu, která se s postupující digitalizací a rozvojem technologií stále více rozšiřuje a přizpůsobuje novým podmínkám.

3.1 Phishing

Phishing je jednou z nejčastějších a nejefektivnějších metod využívaných v sociálním inženýrství. Tento druh útoku spočívá v tom, že útočník předstírá identitu důvěryhodné organizace nebo osoby a prostřednictvím e-mailů, textových zpráv nebo sociálních sítí se snaží oběť přimět k poskytnutí citlivých údajů nebo ke kliknutí na škodlivý odkaz. Mezi tyto údaje patří zejména přihlašovací údaje, čísla kreditních karet, nebo dokonce rodné číslo či adresa. [2] [9] [32]



Obrázek 2 Ukázka phishingového útoku

(zdroj: NECHVÁTAL, Šimon. *Lekce 14 - Kybernetické útoky zaměřené na odcizení citlivých údajů*. Online. Itnetwork.cz. Dostupné z: <https://www.itnetwork.cz/bezpecnost/kyberneticke-utoky-zamerene-na-odcizeni-citlivych-udaju>. [cit. 2025-05-13].)

Phishing není pouze statickou technikou – jeho formy a metody se neustále vyvíjejí, aby dokázal obcházet moderní bezpečnostní systémy. Další podkapitoly budou věnovány tomu, jak phishing funguje, proč je tak efektivní, jaké jsou jeho nejčastější podoby. [33]

3.1.1 Mechanismus phishingových útoků

Podstata phishingu spočívá ve využití poznatků z lidské psychologie. Útočníci cílí na přirozené reakce obětí, jako jsou důvěřivost, strach nebo zvědavost. [16] [33] Většina phishingových útoků pracuje s těmito prvky:

- Napodobení legitimní organizace: Útočníci vytvoří e-maily, webové stránky nebo texty, které jsou vizuálně i jazykově velmi podobné oficiálním materiálům.

Například falešné e-maily od banky budou mít podobné logo, design i formát, aby co nejvíce připomínaly legitimní komunikaci. [2] [10] [28]

- Vytvoření naléhavé situace: Phishingové zprávy často obsahují naléhavé výzvy, jako „Okamžitě ověřte svůj účet, jinak bude zablokován“ nebo „Vaše platba nebyla úspěšná, klikněte zde pro další informace“. Tyto taktiky mají za cíl vyvolat stres a donutit oběť jednat rychle, aniž by si důkladně ověřila legitimnost zprávy. [16] [34]
- Falešné odkazy a přílohy: Útočníci často využívají odkazy na podvodné webové stránky nebo přílohy obsahující škodlivý software. Po kliknutí na odkaz je oběť přesměrována na web, který vypadá jako legitimní stránka, ale slouží k odcizení přihlašovacích a platebních údajů nebo instalaci malwaru. [3] [10] [25] [35]

3.1.2 Formy phishingu

Phishing má mnoho podob, které se liší podle způsobu komunikace a cílové skupiny. [27]

Mezi nejčastější patří:

- E-mailový phishing: Jedná se o klasickou formu phishingu, kdy útočník rozesílá e-maily napodobující legitimní organizace. Tyto e-maily obsahují falešné odkazy nebo přílohy. Například oběť obdrží e-mail údajně od své banky s výzvou k ověření účtu. Po kliknutí na odkaz je oběť přesměrována na falešnou přihlašovací stránku. [16] [22]
- Spear phishing: Na rozdíl od běžného phishingu, který je hromadně rozeslán na široké publikum, spear phishing cílí na konkrétní osoby nebo organizace. Útočník si oběť důkladně prostuduje, například prostřednictvím sociálních sítí, aby vytvořil podvodnou zprávu na míru. Tato forma phishingu je obzvláště nebezpečná a účinná, protože z důvodu personalizace působí velmi přesvědčivě. [2] [10]
- Clone phishing: Tento typ phishingu spočívá v tom, že útočník vytvoří kopii legitimní zprávy (například e-mailu), ale pozmění odkazy nebo přílohy tak, aby vedly na škodlivé stránky. Zpráva vypadá na první pohled důvěryhodně, což zvyšuje pravděpodobnost, že oběť klikne na škodlivý odkaz. [36]
- Whaling: Tento termín označuje phishingové útoky zaměřené na vysoce postavené osoby v organizacích, jako jsou ředitelé nebo manažeři. Útočníci se snaží využít autority těchto osob k získání přístupu k důležitým informacím nebo systémům. [31]

3.2 Pretexting

Pretexting je jednou z pokročilých technik sociálního inženýrství, která se zaměřuje na vytvoření přesvědčivého příběhu za účelem získání citlivých informací od oběti. Na rozdíl od plošných útoků, jako je phishing, vyžaduje pretexting důkladnější přípravu a cílený přístup. Útočník se obvykle vydává za osobu s oprávněním požadovat určité informace, například pracovníka banky, policistu či IT specialistu. Věrohodnost celé situace je klíčem k úspěchu této techniky. [2] [10]

Útočníci využívají nejen manipulace emocí, jako je strach, odpovědnost nebo naléhavost, ale také reálné detaily, které mohou o oběti získat předem z veřejných zdrojů nebo dříve provedených útoků. Příklad může být falešný hovor z banky, kdy útočník tvrdí, že potřebuje potvrdit údajnou podezřelou transakci, a při tom získá přístupové údaje k účtu oběti. Jiným scénářem je podvodný technik IT, který kontaktuje zaměstnance a žádá heslo k firemním systémům pod záminkou jejich údržby. [9] [31] [37]

3.2.1 Princip a účinnost pretextingu

Pretexting spoléhá na dvě klíčové strategie: vytvoření důvěryhodného příběhu a manipulaci emocí oběti. Útočník se například může představit jako pracovník autoritativní instituce (banka, policie, státní správa) a použít specifické informace o oběti, aby zvýšil důvěryhodnost. Oběť pak na základě pocitu povinnosti nebo naléhavosti ochotně poskytne požadované údaje. [10] [31]

Hlavními faktory úspěchu jsou:

- Personalizace: Útočník často využívá konkrétní informace o oběti, jako je její jméno, adresa nebo pracovní pozice, aby zvýšil autenticitu.
- Emoční tlak: Naléhavé situace, například „bezprostřední riziko ztráty peněz“, snižují schopnost oběti logicky uvažovat.
- Nedostatek ověřování: Lidé mají tendenci důvěřovat institucím a neověřují pravost požadavků, zvláště pokud je na ně vyvíjen tlak. [10] [31]

3.3 Baiting

Baiting je technika sociálního inženýrství, která využívá lidské zvědavosti nebo touhy po odměně. Útočníci manipulují oběti pomocí atraktivních nabídek nebo situací, aby získali

přístup k jejich citlivým datům nebo infikovali jejich zařízení škodlivým softwarem. [20] [27] [31]

Jedním z běžných příkladů baitingu je zanechání USB disku na veřejném místě, například v kanceláři nebo kavárně. Oběť, kterou zaujme obsah disku, jej připojí ke svému počítači, čímž umožní útočnickovi spustit škodlivý kód nebo získat přístup k systému. Na internetu se baiting často objevuje ve formě falešných nabídek, jako jsou nelegální filmy nebo software zdarma, které ve skutečnosti obsahují malware. [3] [27] [31]

Daný typ útoku je nebezpečný zejména proto, že spoléhá na přirozené lidské chování a zvědavost. Lidé se často cítí přesvědčení, že riskovat se vyplatí, zejména pokud očekávají, že něco získají. Přitom si neuvědomují rizika spojená s neopatrným jednáním, jako je infikování zařízení, ztráta dat nebo dokonce krádež identity. [10] [13] [31]

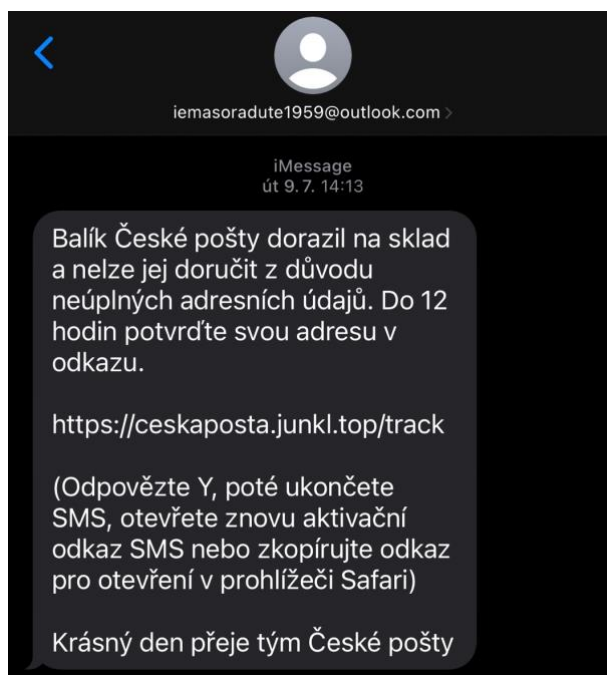
3.4 Vishing

Jedná se o techniku sociálního inženýrství, která se zaměřuje na získání citlivých informací prostřednictvím telefonních hovorů nebo hlasových zpráv. Útočníci se často vydávají za pracovníky důvěryhodných institucí, jako jsou banky, úřady nebo poskytovatelé služeb, a nutí oběť k poskytnutí osobních údajů a citlivých informací. [10] [22]

Tento typ útoku je obzvláště účinný na starší generaci, která může mít nižší povědomí o bezpečnostních hrozbách a může být zvyklá komunikovat prostřednictvím telefonu. Starší lidé bývají více náchylní k důvěřování autoritám a mohou snadněji podlehnout falešným tvrzením. Vishing tedy představuje závažnou hrozbu pro tuto věkovou skupinu. [10] [17] [19]

3.5 Smishing

Smishing (SMS phishing) je forma sociálního inženýrství, při které útočník používá textové zprávy (SMS) k získání citlivých informací od oběti. Tyto zprávy často obsahují odkazy na falešné webové stránky, které se tváří jako legitimní stránky bank, e-shopů nebo jiných důvěryhodných institucí. Oběť je v těchto zprávách vyzvána, aby klikla na odkaz a zadala své přihlašovací údaje, čísla kreditních karet nebo jiné citlivé informace. [4] [16] [31]



Obrázek 3 Smishingový útok

(zdroj: vlastní)

Daný útok je účinný, protože mnoho lidí je zvyklých důvěřovat textovým zprávám, zejména pokud pocházejí od známých nebo autoritativních institucí. Útočníci často vytvářejí zprávy, které mají urgentní tón nebo obsahují lákavé nabídky, což oběť motivuje k okamžitému jednání, aniž by si ověřila pravost zprávy. Tento typ útoku je efektivní, protože SMS zprávy mohou vypadat na první pohled důvěryhodně a oběť nemusí být dostatečně obezřetná při ověřování odkazu. [3] [12] [31]

4 STARŠÍ GENERACE

Věřejnost si často nesprávně spojuje pojmy senior a důchodce, přestože mají zcela odlišný význam. Senior je širší označení pro osobu v pokročilém věku, zatímco důchodcem je jedinec, který pobírá důchod z důvodu věku nebo invalidity.

V rámci legislativy je za seniora považována žena od 60 let a muž od 63 let. Některé instituce však uvádějí hranici 55 let. Obecně se ale seniorem rozumí osoba starší 60 let bez ohledu na pohlaví. [38]

Starší lidé mohou být rozděleni do tří hlavních věkových skupin, přičemž s rostoucím věkem se zpravidla zhoršují kognitivní schopnosti a schopnost objektivně vyhodnotit situaci, což ovlivňuje jejich odlišnou zranitelnost vůči sociálnímu inženýrství:

1. Věková skupina 60–69 let

Tato skupina zahrnuje lidi, kteří jsou většinou aktivní, často ještě pracují, nebo jsou v předdůchodovém věku. Mnozí mají relativně dobrou úroveň technologických dovedností, ale stále čelí výzvám ve zpracování nových technologií a rychlým změnám v digitálním světě. Zranitelnost je dána zejména důvěřivostí k novým příležitostem, jako jsou investice nebo nabídky, které znějí příliš dobře na to, aby byly pravdivé. I přes určitou zkušenost mohou být náchylní k manipulaci, pokud se podvodník přizpůsobí jejich preferencím a způsobu komunikace.

2. Věková skupina 70–79 let

Tato skupina představuje starší lidi, kteří jsou již většinou v důchodu. Mohou mít omezený přístup k novým technologiím a jsou často méně zdatní při rozpoznávání hrozeb na internetu nebo v každodenním životě. Většina těchto lidí je méně ochotná se přizpůsobovat rychlým technologickým změnám, což je činí zranitelnějšími vůči podvodům, které využívají staré ověřené taktiky, jako je telefonování, poštovní podvody a podvodné nabídky na pomoc nebo zdravotní péči.

3. Věková skupina 80 a více let

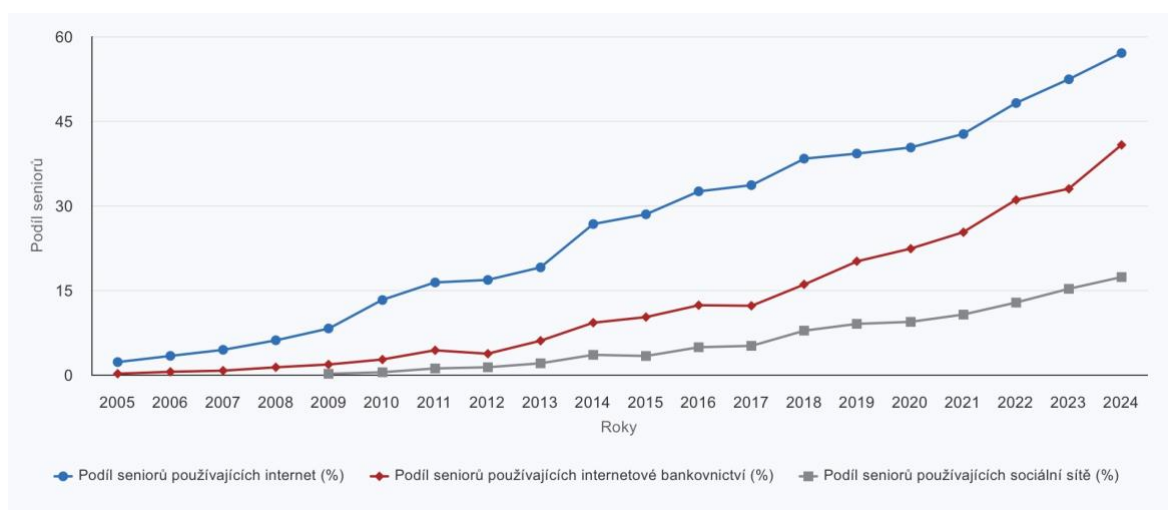
Tato skupina zahrnuje osoby ve vysokém věku, často s vážnými zdravotními problémy, jako je zhoršená paměť, demence nebo jiná kognitivní onemocnění. Tito lidé jsou nejvíce zranitelní vůči podvodníkům, kteří využívají jejich osamělost, slabší kognitivní schopnosti a omezenou schopnost rozpoznat podvodné praktiky. Mohou

být snadno zmanipulováni emocionálními taktikami a nátlakem, které je přesvědčí k poskytnutí osobních nebo finančních informací. [37] [39] [40]

4.1 Senioři a informační technologie

Zatímco mladší generace vyrůstaly v prostředí digitálních technologií, starší lidé s nimi přicházejí do kontaktu až v pozdějším věku. Právě proto je sledování jejich přístupu k informačním technologiím, jako jsou počítače, mobilní zařízení nebo internet, důležité i z hlediska demografického vývoje. Výběrová statistická šetření poskytují přehled o tom, jak se tyto technologie šíří i mezi seniory.

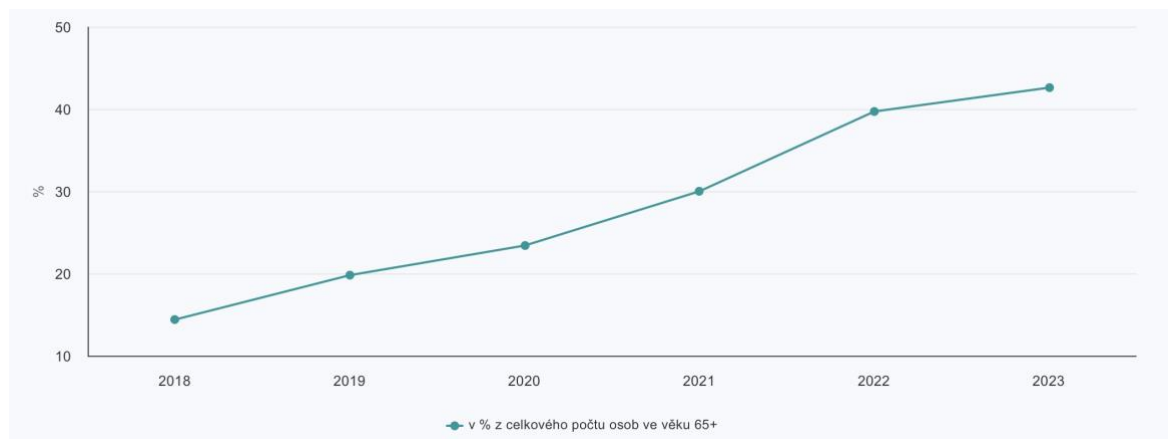
Mezi seniory dominuje při používání počítačových zařízení notebook, následovaný stolním počítačem. V roce 2023 jej využívalo 30 % osob ve věku 65 a více let, stolní počítač 25 % a tablet 9 %. Oproti roku 2016 se zvýšilo zastoupení všech tří zařízení v domácnostech seniorů. Zájem o internet u seniorů roste – v roce 2006 jej používalo jen 3 % osob starších 65 let, v roce 2023 již 65 % ve věku 65–74 a 34 % ve věku 75 a více let. Výrazně přibýlo i seniorů používajících sociální sítě a internetové bankovníctví. [41]



Graf 2 Podíl seniorů, využívajících moderní technologie

(zdroj: *Využívání PC a internetu. Senioři v datech [online]. [vid. 2025-05-04]. Dostupné z: <https://csu.gov.cz/seniori-v-datech/vyuzivani-pc-a-internetu>*)

Podíl seniorů využívajících mobilní telefon vzrostl z 90 % v roce 2018 na 96 % v roce 2023. Významně se proměnila i struktura užívaných zařízení – tradiční tlačítkové telefony ustoupily modernějším smartphonům, které v roce 2023 používalo 54 % seniorů oproti pouhým 14 % v roce 2018. [41]



Graf 3 Podíl seniorů, využívajících chytrý telefon

(zdroj: *Využívání PC a internetu. Senioři v datech [online]. [vid. 2025-05-04]. Dostupné z: <https://csu.gov.cz/seniori-v-datech/vyuzivani-pc-a-internetu>)*

4.2 Aktivity starší generace v kyberprostoru

Nejčastějšími činnostmi, které senioři ve věku 65 a více let na internetu v roce 2023 vykonávali, bylo čtení zpráv, používání e-mailu a vyhledávání informací o zboží. Tyto aktivity vykazují dlouhodobou stabilitu, přestože v roce 2015 byl jejich výskyt zhruba poloviční. Nižší zastoupení má mezi seniory využívání sociálních sítí, přičemž věková struktura ukazuje na významné rozdíly: zatímco ve věkové skupině 65-74 let je využívalo 21 %, ve skupině 75 a více let pouze 7 %. Z dalších činností lze uvést, že 37 % seniorů vyhledávalo informace o zdraví, 33 % využívalo internetové bankovníctví a 27 % nakupovalo online. Právě online nakupování zaznamenalo prudký nárůst během pandemie v roce 2020 a jeho obliba u starších uživatelů zůstala i v následujících letech. [41]

4.3 Senioři jako snadný cíl sociálního inženýrství

Ve vztahu ke kriminalitě je nutné považovat seniory za zvláštní kategorii, a to jak na straně obětí, tak v některých případech i pachatelů. Dlouhodobě patří mezi nejvíce zranitelné skupiny, přičemž tuto zranitelnost dále prohlubuje kriminalita, která se odehrává v digitálním prostředí. Od 1. dubna 2017 zákon o obětech trestných činů uznává seniory jako „zvlášť zranitelné oběti“. [37] [40]

Důvody, proč se právě senioři stávají častým cílem kybernetických útoků využívajících metody sociálního inženýrství, lze shrnout do následujících bodů:

- Nízká digitální gramotnost: Podvodníci spoléhají na to, že senioři nejsou plně obeznámeni s fungováním digitálních technologií a často postrádají jistotu v kyberprostoru. Snížená schopnost rozpoznat širší souvislosti pak přispívá k jejich vyšší zranitelnosti vůči manipulacím. [37] [42]
- Finanční situace a obavy z úspor: Senioři s pravidelným důchodem a naspořeným jměním mohou být atraktivním cílem pro podvodníky právě díky své stabilní finanční situaci. Pachatelé často zneužívají obav seniorů ze ztráty finančních prostředků, čímž je manipulují k impulzivnímu jednání, například k odeslání peněz nebo sdělení citlivých údajů. Příkladem je scénář s tzv. „falešným bankéřem“, kdy se pachatelé vydávají za autority a snaží se seniory vystrašit tvrzením, že jejich úspory jsou v nebezpečí a musí okamžitě jednat, aby je ochránili. [37] [40]
- Zhoršení kognitivních funkcí a zdravotního stavu: Vysoký věk často přináší specifické problémy, a to zejména zdravotní a mentální, které činí seniory zranitelnějšími. Podvodníci využívají jejich nižší odolnost a oslabenou schopnost účinně reagovat na nebezpečné situace. Mezi faktory, které zvyšují zranitelnost seniorů, patří pokles životní energie, oslabení sociálních dovedností, projevy nepozornosti a nízké ostražitosti, známky duševní nepohody či onemocnění, tělesná slabost a sociální izolace. [39] [40]
- Neochota přiznat chybu: Senioři se mnohdy stydí přiznat, že se stali obětí podvodu. Obavy z odsouzení nebo ztrapnění je vedou k tomu, že si situaci nechávají pro sebe a nesvěřují se ani členům rodiny. Tato uzavřenost ztěžuje včasnou pomoc a přispívá k nižší míře oznamování těchto trestných činů. Je proto zásadní, aby osvěta cílila také na odbourání tohoto ostychu a povzbudila seniory k tomu, aby o podvodu mluvili a nebáli se požádat o pomoc. [40] [43]

4.4 Zranitelnost starší generace vůči kybernetickým podvodům a strategie prevence

Všechny věkové skupiny starších lidí sdílejí určité zranitelnosti, které podvodníci využívají. Mezi nejčastější faktory, které zvyšují jejich zranitelnost, patří psychologické a emocionální potřeby. Starší lidé bývají často osamělí, což je činí náchylnějšími k manipulativní komunikaci, která jim slibuje společnost, pomoc nebo ochranu. Technologická gramotnost

také hraje klíčovou roli, jelikož mnozí starší lidé nejsou obeznámeni s novými technologiemi ani s tím, jak se chránit před hrozbami v kyberprostoru. [19] [43]

Prevence by měla zahrnovat několik základních přístupů:

- **Vzdělávání a osvěta:** Starší lidé potřebují jednoduše podané informace o bezpečnosti v kyberprostoru a o nejčastějších podvodních praktikách. Mohou být například varováni, jak poznat phishingové e-maily nebo telefonáty od „falešných“ úředníků. Také je důležité je vzdělávat o ochraně osobních údajů, například při používání platebních karet a bankovních účtů. [17] [19] [44]
- **Technická podpora:** Zajištění základních nástrojů pro ochranu soukromí, jako jsou bezpečné hesla a dvoufaktorová autentizace, může pomoci chránit starší osoby před podvodným jednáním. Mohou také využívat speciální software pro blokování nežádoucí komunikace. [19] [25] [45]
- **Bezpečnostní opatření pro finanční transakce:** Starší lidé by měli být informováni o tom, jak ověřit důvěryhodnost finančních transakcí a o tom, že by neměli poskytovat své bankovní údaje ani PINy přes telefon nebo e-mail. [19]
- **Osobní a pravidelná komunikace:** Pravidelný a osobní kontakt s osobami vyššího věku ze strany rodinných příslušníků, přátel nebo opatrovníků je zásadní nejen pro včasné rozpoznání podezřelého chování, ale také pro předávání důležitých informací a společné konzultace situací, v nichž si senioři nemusí být jisti správným postupem.

Národní úřad pro kybernetickou a informační bezpečnost vytvořil pomůcku s názvem SENIOR, která je určena k snadnějšímu rozpoznávání podezřelých zpráv a podvodných technik, které útočníci na internetu často využívají. Název je tvořen z počátečních písmen slov „soubory“, „emoce“, „nátlak“, „instrukce“, „odkazy“ a „reputace“, které představují typické nástroje využívané internetovými podvodníky. Tato slova dohromady tvoří akronym SENIOR, jenž zároveň slouží jako pomůcka pro zapamatování. Uživatelům je k dispozici šest klíčových otázek, které mohou výrazně napomoci k rozpoznání podvodného jednání. Konkrétně se jedná o následující otázky:

„Je ke zprávě přiložený soubor, který máte stáhnout a otevřít?“

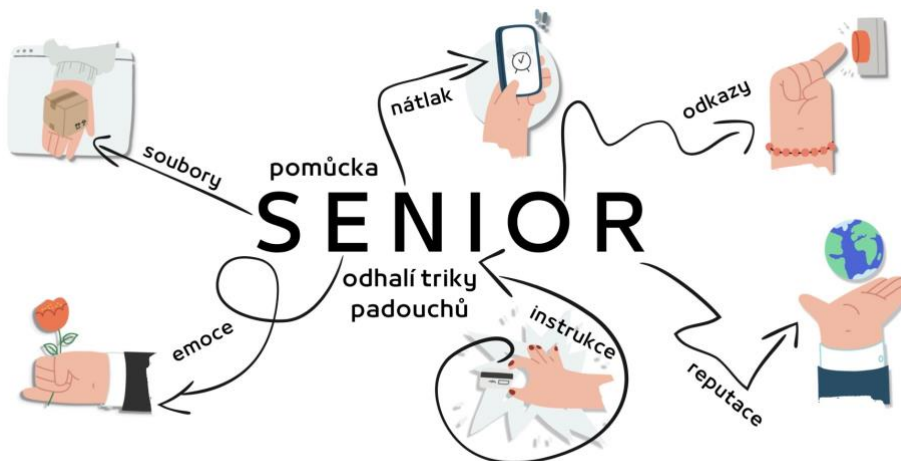
„Vzbuzuje zpráva emoce jako strach, překvapení nebo zvědavost?“

„Snaží se vás zpráva dostat pod tlak a do časové tísně?“

„Poskytuje zpráva konkrétní instrukce a návody, které máte vykonat?“

„Je ve zprávě odkaz, kterému máte věnovat pozornost?“

„Posílá zprávu autoritativní instituce nebo osoba?“ [46]



Obrázek 4 Pomůcka SENIOR

(zdroj: Pomůcka SENIOR [online]. [vid. 2025-05-04]. Dostupné
z: <https://osveta.nukib.gov.cz/senior>)

Preventivní strategie musí reflektovat individuální schopnosti a potřeby různých věkových kategorií. Je nezbytné, aby informace zaměřené na prevenci byly formulovány srozumitelně, přehledně a bez zbytečné technické náročnosti, aby i osoby s nižší digitální gramotností či zdravotním omezením dokázaly včas identifikovat pokusy o sociální manipulaci a adekvátně na ně reagovat.

II PRAKTICKÁ ČÁST

5 ANALÝZA KONKRÉTNÍCH PODVODŮ ZAMĚŘENÝCH NA SENIORY

Podvody zaměřené na starší generace představují závažný společenský problém, který se v posledních letech výrazně rozšiřuje s rozvojem technologií a online prostředí. Starší generace se často stává cílem podvodníků kvůli jejich omezené znalosti digitálních technologií, důvěřivosti a slabšímu povědomí o hrozbách kybernetické kriminality. Tato kapitola se zaměřuje na konkrétní případy podvodů páchaných na seniorech, přičemž cílem je podrobná analýza použitého modus operandi pachatelů a určení preventivních opatření, která by mohla podobným situacím předcházet. Analýza jednotlivých případů nejen ilustruje kreativitu podvodníků, ale také poukazuje na zranitelnosti, na které je třeba se v prevenci zaměřit. [37]

5.1 Inzerát na internetu

Případ z Benešovska ukazuje, jak mohou podvodníci využívat důvěřivosti starších lidí při online transakcích. 68letý muž nabízel na inzertním portálu krbové vložky za cenu 3000 Kč. Kontaktoval ho údajný zájemce, který místo běžné platby poslal odkaz na webovou stránku, která se tvářila jako služba přepravní společnosti. Senior na této stránce zadal údaje ke své platební kartě včetně aktivačního klíče, načež mu z účtu zmizelo téměř 80 000 Kč

Muž si však podvodu záhy všiml a případ nahlásil policii, která zahájila trestní řízení. Pachatelovi v případě dopadení hrozí až dva roky odnětí svobody. [47]

Případ je varovným příkladem, jak snadno mohou být starší lidé vystaveni kybernetickým hrozbám. Scénář tohoto podvodu odpovídá obvyklým praktikám, kdy útočníci zneužívají inzertní portály k oslovování prodejců. Podvodník vystupuje jako seriózní zájemce, který má o nabízené zboží zájem, a následně navrhne alternativní způsob platby nebo přesměruje oběť na podvodnou stránku. Takové stránky vypadají důvěryhodně a často napodobují známé služby, což oběť snadno oklame. Zadáním údajů o platební kartě podvodník získá přístup k finančním prostředkům na účtu oběti.

V tomto případě senior mohl postupovat bezpečněji. Základní pravidlo zní, že kupující by měl peníze posílat přímo na účet prodávajícího, a nikoli požadovat zadání platebních údajů na jiné stránce. Pokud by senior odkaz ignoroval a konzultoval situaci například se známými nebo zaměstnanci banky, mohl by se podvodu vyhnout. Důležitá je také

obezřetnost při používání internetových služeb, nikdy neklikat na podezřelé odkazy a nezadávat citlivé údaje na stránkách, které nejsou ověřené.

Senior by se měl řídit těmito jednoduchými pravidly: neklikat na neověřené odkazy, nesdělovat citlivé údaje o platební kartě a vždy ověřovat identitu druhé strany. Tímto způsobem lze výrazně snížit riziko, že se stane obětí podobných podvodů. Tento případ by měl být varováním nejen pro seniory, ale i pro jejich rodiny a blízké, aby věnovali pozornost bezpečnostním návykům svých příbuzných a pomáhali jim s orientací v online prostředí. [37]

Podobné případy naznačují nezbytnost vzdělávání a prevence. Policie ČR i banky pravidelně varují před různými typy podvodů, ale klíčová je cílená osvěta zaměřená na seniory. Ti často nemají dostatečné zkušenosti s moderními technologiemi a mohou být snadno oklamáni. Prevence by měla zahrnovat pravidelné informování o aktuálních, neustále se vyvíjejících podvodech, jasné instrukce, jak se chránit, a posilování povědomí o základních zásadách kybernetické bezpečnosti.

5.2 Případ vishingu z Děčína

V říjnu 2024 se na Děčínsku stal pětáosmdesátiletý muž obětí propracovaného internetového podvodu, který ho připravil o více než 600 000 Kč. Případ začal telefonátem, kdy neznámý volající seniorovi oznámil, že má údajně na účtu kryptoměny v hodnotě přibližně 100 000 Kč, a nabídl mu možnost jejich vyplacení či zhodnocení. Senior si vzpomněl, že v minulosti skutečně kryptoměny vlastnil, čehož podvodník mistrně využil a zahájil proces manipulace pomocí technik sociálního inženýrství.

Podvodník se vydával za profesionála a používal tzv. spoofovaná telefonní čísla, která se jevila jako česká, ale ve skutečnosti pocházela ze zahraničí. Postupně přesvědčil seniora, aby si do svého počítače nainstaloval programy pro vzdálenou správu. Útočník tímto získal přístup k zařízení oběti, včetně možnosti sledovat její aktivitu v online bankovníctví. Senior následně odeslal v několika platbách na různé účty přes 600 000 Kč v domněnání, že jde o investice do kryptoměn. Po několika dnech si uvědomil, že se stal obětí podvodu, a kontaktoval policii. Rychlá reakce kriminalistů umožnila zajistit část odeslaných peněz, nicméně podvodník zatím zůstává neznámý. V případě jeho dopadení mu hrozí až pět let vězení za trestný čin podvodu. [48]

Podvodníci v takových případech využívají kombinaci psychologického nátlaku a technologických nástrojů, aby oběť zmanipulovali k rychlému a často neuváženému jednání. Oběti bývají zahlceny množstvím informací, což snižuje jejich schopnost kriticky uvažovat a hledat nezávislé ověření předkládaných tvrzení.

V tomto konkrétním případě mohl senior předejít ztrátě peněz několika způsoby. Především by měl vždy zpochybnit informace, které obdrží od neznámých volajících, zejména pokud se týkají financí. Konzultace s rodinou, přáteli nebo odborníky by mohla přinést potřebnou perspektivu a odhalit podvod. Instalace softwaru na vzdálenou správu je vždy podezřelá a riziková, pokud k ní vyzve neznámá osoba, je nezbytné takový požadavek odmítnout. Dále je důležité věnovat pozornost telefonátům z neznámých čísel, přičemž zpětné volání na podezřelé číslo může často potvrdit, že se jedná o spoofing. [7] [17]

Klíčovým momentem je také zvládnutí psychického nátlaku. Podvodníci spoléhají na to, že oběť bude jednat impulzivně, pod tlakem a bez dostatečného rozmyslu. Odmítnutí jednat okamžitě a vyžádání času na rozmyšlenou je zásadní. Vždy je také třeba ověřit si informace přímo u banky, případně kontaktovat policii v případě podezření na podvodné jednání.

Tento případ podtrhuje význam prevence, která spočívá zejména ve vzdělávání seniorů a jejich blízkých. Důležitá je pravidelná komunikace, sdílení informací o aktuálních rizicích a budování kritického přístupu k nevyžádaným nabídkám. Osobní obezřetnost a ochota konzultovat neobvyklé situace mohou být účinným nástrojem, jak se těmto podvodům vyhnout. Každý krok směrem k vyšší informovanosti a pozornosti může pomoci předejít nejen finanční ztrátě, ale také psychickým dopadům, které podobné situace často způsobují.

5.3 Případ vishingu z Tábořska

V období od konce února do 6. března 2023 se stal senior z Tábořska obětí podvodného jednání při pokusu o investici do kryptoměn. Podvodník kontaktoval poškozeného a nabídl mu výhodnou investiční příležitost. Poškozený se zaregistroval prostřednictvím zaslaného formuláře a uhradil registrační poplatek. Poté, co podvodník navázal telefonní kontakt, požádal poškozeného o nainstalování programu AnyDesk pro vzdálený přístup k jeho počítači. Když podvodník získal přístup k zařízení oběti, přihlásil se do jejího internetového bankovníctví a přiměl ji, aby autorizovala několik plateb. Poškozený odeslal více než 200 000 Kč na neznámý účet, přičemž transakce byly schváleny pomocí SMS kódů.

Policie ČR varuje, že vyšetřování podobných podvodů je často složité a zdlouhavé, a že ne vždy se podaří pachatele dopadnout. Ve virtuálním prostoru lidé často ztrácejí ostražitost a nechávají se podvodníky snadno zmanipulovat. Výsledkem bývá zpravidla ztráta vysokých finančních částek, které jsou následně převezeny na neznámé účty, často v zahraničí. [49]

Tento případ jasně ukazuje nebezpečí, která číhají na každého, kdo se rozhodne investovat do kryptoměn nebo jiných online investičních příležitostí. Při investování si je vždy potřeba zjistit co nejvíce informací o dané burze, platformě nebo investiční nabídce. Je vhodné si vyhledat recenze a reference od jiných uživatelů a ověřovat si legitimitu poskytovatele investic. [19] [21]

V případě jakéhokoli telefonického kontaktu s cizími osobami je potřeba být velmi obezřetný, nikdy nesdělovat své osobní údaje, informace o platebních kartách, kódy nebo hesla, které by umožnily vzdálený přístup k vašemu počítači nebo účtům. Pokud vám někdo cizí nabídne vzdálený přístup k vašemu počítači, okamžitě tento požadavek odmítněte. Také se vyhněte tomu, abyste ve chvílích, kdy je k vašemu počítači připojen někdo cizí, prováděli přihlášení do internetového bankovníctví. Dále je důležité, abyste nikdy nesdíleli nebo neposílali autorizační SMS kódy, které vám dorazí od banky. [19] [45]

Pro zvýšení bezpečnosti je potřeba mít na počítači nainstalován aktualizovaný antivirový program a v internetovém bankovníctví nastavené co nejnižší limity pro platby. Tyto limity je vhodné zvyšovat pouze na nezbytně nutnou částku pro konkrétní platbu. Pokud se přesto stanete obětí podobného podvodu, je žádoucí okamžitě informovat Policii ČR prostřednictvím tísňové linky 158 nebo na jakékoliv policejní služebně. Je také důležité informovat svůj bankovní ústav a zálohovat veškerou komunikaci s podvodníkem, která následně bude předložena vyšetřovatelům.

V případě, že by senior dodržoval tato pravidla, velmi pravděpodobně by včas rozpoznal podvodný charakter situace a předešel by finanční ztrátě.

5.4 Případ podvodu při investování

V létě 2024 se na policii obrátil 73letý senior z Olomoucka, který přišel o značnou částku peněz v důsledku podvodného investičního programu. Vše začalo, když muž obdržel SMS zprávu s lákavou nabídkou na výhodnou investici do komodit s využitím umělé inteligence, která slibovala vysoké zisky. Senior, přestože byl upozorněn na možná rizika, na zprávu

zareagoval, klikl na odkaz a zaregistroval se. Po registraci byl požádán o vklad počáteční částky 5 500 Kč, což učinil, a následně byl telefonicky kontaktován údajným finančním poradcem, který mu poskytl instrukce ohledně investic.

Po několika týdnech, kdy muž sledoval na grafu rostoucí zisky, souhlasil s navýšením investice o 2 600 EUR, jak mu radil poradce. Podvodník se zaměřil na přesvědčování seniora, že investice do ropy, zlata a zahraniční měny přinesou rychlý zisk. Po několika týdnech mu bylo nabídnuto si vybrat 12 000 dolarů z investic, ale když muž o převod peněz požádal, byl informován, že převod blokuje zahraniční společnost, která požaduje vratnou zálohu 3 600 dolarů. Senior, stále věřící ve slibovaný zisk, zaplatil i tuto částku, ale peníze na jeho účet stále nepřišly. O měsíc později mu byla nabídnuta další platba na úhradu 15% daně, což už však odmítl. V tu chvíli komunikace s poradcem skončila.

Podvodník následně zřejmě změnil strategii a seniora kontaktovala jiná osoba, tentokrát „finanční poradkyně“. Opět mu byla nabídnuta investice, tentokrát s počátečním vkladem 10 000 Kč, přičemž mu byla slibována denní výplata 7 dolarů. Po několika dnech mu byla nabídnuta investice ve výši 103 000 Kč s možností výdělku až 60 000 Kč měsíčně. Po několika dalších týdnech, když si senior přál vybrat 450 dolarů, zjistil, že peníze znovu neobdržel, a poradkyně přestala komunikovat.

Muž přišel o 260 000 Kč, což byla částka, kterou investoval s očekáváním rychlého a vysokého zisku. Teprve poté, co v televizním pořadu zahlédl reportáž o podobných případech, si uvědomil, že byl podveden. Následně podal oznámení na policii, která zahájila trestní řízení. [50]

Podvodníci v tomto případě využili kombinace psychologického nátlaku, technologických nástrojů a důvěryhodně vypadající komunikace (SMS zpráva, telefonní hovory, grafy zisků), aby seniora přiměli k opakovaným investicím.

Podvodník nejprve využil lákavou nabídku výhodné investice, která slibovala vysoký zisk, který měl seniora motivovat k rychlé reakci bez důkladného prověření. Tento slib vysokých výnosů je jedním z hlavních charakteristik podvodných investic a je často používán k manipulaci. Důležitým prvkem tohoto podvodu byla komunikace s „finančním poradcem“, který působil jako odborník na investice. Poradci jsou často zneužíváni podvodníky k tomu, aby navodili dojem důvěryhodnosti a expertízy, což seniory uklidňuje a přesvědčuje je o správnosti jejich rozhodnutí. Poradci podali konkrétní pokyny ohledně investování, což mělo posílit dojem serióznosti celé transakce.

Po úspěchu prvního podvodu podvodníci změnili strategii a předali komunikaci jiné osobě, která měla být „finanční poradkyní“. Tento krok je součástí snahy podvodníků minimalizovat riziko odhalení tím, že změní identitu, čímž ztěžují odhalení jednotlivých částí podvodu. To ukazuje, jak podvodníci dokážou měnit taktiky podle potřeby, aby se vyhnuli podezření.

Senior, i přes opakovaný kontakt s podvodníkem, nezaznamenal žádné výrazné varovné signály, které by ho přiměly k opatrnosti. Podvodník v tomto případě zvolil taktiku postupného zvyšování psychologického tlaku a přesvědčování o výhodnosti investice s potenciálem vysokého zisku. Podvodníci často využívají psychologickou manipulaci, aby oběti ztratily svou přirozenou ostražitost a učinily rozhodnutí, která by za normálních okolností vyhodnotily jako podezřelá.

Aby se senior vyhnul ztrátě úspor, měl by v podobné situaci učinit několik preventivních kroků. Klíčové je důkladné ověření důvěryhodnosti investice a subjektu, který ji nabízí. Lákavé nabídky s vysokým výnosem bývají často součástí podvodného schématu. Je důležité nezasílat peníze na neověřené účty a nenechat se tlačit do rychlého rozhodnutí. Rovněž je třeba ověřit kvalifikaci osob, které poskytují investiční poradenství, neboť podvodníci se často vydávají za odborníky s falešnými identitami.

V žádném případě by neměl senior hradit poplatky za výplatu výnosů nebo jiné údajné administrativní náklady, pokud si jejich oprávněnost nemůže ověřit. Pokud nabídka vyvolává pochybnosti, měl by se obrátit na důvěryhodné osoby ve svém okolí nebo odborníky v oblasti financí. V případě podezření na podvod je nezbytné okamžitě kontaktovat policii a svou banku, aby bylo možné zabránit dalším finančním ztrátám. Včasné a uvážené jednání může být klíčové pro ochranu úspor.

6 POVĚDOMÍ O SOCIÁLNÍM INŽENÝRSTVÍ U STARŠÍ GENERACE

V rámci praktické části bakalářské práce bylo realizováno dotazníkové šetření zaměřené na zmapování informovanosti starší generace o hrozbách spojených se sociálním inženýrstvím a kybernetickou kriminalitou. Dotazník, sestavený s důrazem na jednoduchost a srozumitelnost, zahrnoval otázky týkající se jak obecných znalostí, tak konkrétních zkušeností respondentů s podvodnými praktikami, jako jsou vishing, phishing či smishing. Výzkum dále sledoval vztah seniorů k moderním technologiím a jejich vnímání bezpečnosti v online prostředí. Šetření přineslo poznatky, které mohou pomoci při navrhování vhodných preventivních opatření.

6.1 Cíl šetření

Cílem dotazníkového šetření je analyzovat úroveň informovanosti seniorů o problematice sociálního inženýrství, zjistit jejich zkušenosti s různými typy podvodného jednání a posoudit, jak bezpečně se cítí při využívání moderních technologií, jako je internetové bankovníctví. Součástí šetření je také snaha odhalit hlavní slabá místa v bezpečnostních návycích starší populace a zhodnotit jejich vnímání rizik spojených s online i telefonickou komunikací. Na základě analýzy výsledků šetření bude navrženo, jakým způsobem efektivně šířit povědomí o rizicích sociálního inženýrství mezi seniory. Zde je znění hlavní výzkumné otázky:

- Jaké je povědomí seniorů o sociálním inženýrství a s ním spojenými hrozbami?

Hypotéza:

- Senioři mají tendenci podceňovat rizika spojená s osobními údaji a věří, že je nikdo nedokáže donutit k jejich odhalení.

6.2 Zpracování šetření

Pro dotazníkové šetření byla zvolena kombinace fyzické a online formy vyplnění dotazníků. Většina respondentů, konkrétně 115, vyplnila dotazník ručně (v papírové podobě), zatímco 7 dotazníků bylo vyplněno prostřednictvím online portálu Survio. Pro seniory je stále vhodnější a pohodlnější vyplňovat dotazníky ručně, což bylo v tomto případě zohledněno. Pro zjednodušení analýzy a přehlednosti byly veškeré dotazníky nahrány do nástroje Google Forms, který umožňuje snadnou práci s daty a jejich následnou analýzu.

Sběr dat probíhal od 1.4. 2025 do 22.04. 2025. Distribuce dotazníku byla zajištěna osobně, a to v klubech a centrech pro seniory, po předchozí domluvě s předsedy těchto zařízení. Online verze dotazníku byla vyplněna jen několika respondenty, kteří preferovali tuto formu. Komunikace se zástupci center pro seniory a klubů seniorů zajistila, že dotazník byl distribuován správné cílové skupině: osobám starším 60 let. Tento výběr respondentů byl klíčový pro správnou realizaci šetření.

Dotazník pro tento výzkum se skládal z 20 otázek, z nichž 5 bylo zaměřeno na demografické údaje účastníků, zatímco dalších 15 se týkalo testování hypotézy a dosažení hlavního výzkumného cíle. Většina otázek byla uzavřených, kde byla k dispozici pouze jedna odpověď, ale u některých otázek bylo možné napsat vlastní odpověď. Na začátku dotazníku byly poskytnuty informace o tématu výzkumu, autorovi a instituci, spolu s pokyny k vyplnění dotazníku. Účastníci byli informováni o účelu dotazníkového šetření a jejich účast byla dobrovolná. Všechny odpovědi jsou anonymní a samotný dotazník je k nahlédnutí v příloze na konci práce.

Pro zajištění kvalitních a validních dat byl dotazník navržen tak, aby byly otázky jasné a srozumitelné pro cílovou skupinu respondentů, tedy seniory. Sběr dat probíhal způsobem, který umožnil získání co nejvíce relevantních informací.

Všem respondentům a těm, kteří se podíleli na distribuci dotazníků, patří mé velké poděkování.

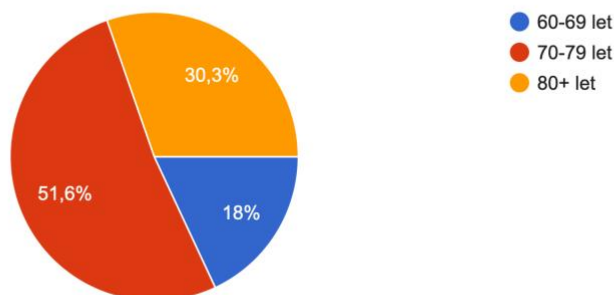
6.3 Cílová skupina a výběr účastníků

Všechny odpovědi byly pečlivě zkontrolovány a vyhodnoceny, přičemž bylo zajištěno, že účastníci splňovali stanovená kritéria pro zahrnutí do výzkumu. Díky správné distribuci dotazníků, která probíhala v klubech seniorů a seniorských centrech, nebylo nutné vylučovat žádné odpovědi na základě věkového kritéria. Veškerá data byla analyzována bez nutnosti odstranění odpovědí v souvislosti s věkem, což potvrzuje efektivní volbu distribučních kanálů. Celkový vzorek respondentů tedy odpovídal požadavkům výzkumu a všechna získaná data byla považována za relevantní pro další analýzu.

První otázka dotazníku se zaměřila na věk respondentů. Největší podíl, konkrétně 51,6 %, tvořili respondenti ve věkové kategorii 70–79 let. Druhou nejpočetnější skupinou byli respondenti ve věku 80 a více let, kteří představovali 30,3 % vzorku. Zbývajících 18 % respondentů spadalo do věkové kategorie 60–69 let. Viz Graf 4.

1. Věk

122 odpovědí



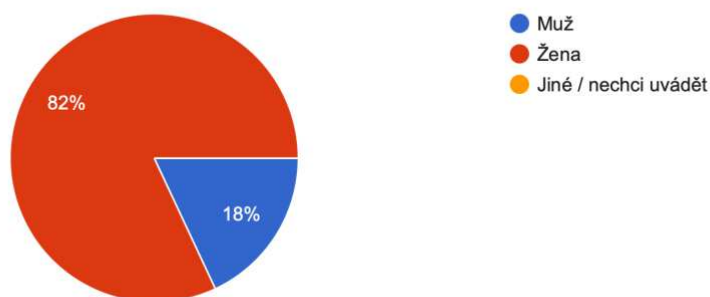
Graf 4 Věk respondentů

(zdroj: vlastní)

Druhá otázka dotazníku se věnovala pohlaví respondentů. Výsledky ukázaly, že většinu tvořily ženy, které reprezentovaly 82 % vzorku, zatímco muži tvořili pouze 18 %. Tento disproporční podíl může odrážet větší zájem a ochotu žen zúčastnit se výzkumu zaměřeného na problematiku sociálního inženýrství a kybernetické bezpečnosti. Grafické znázornění této distribuce pohlaví je uvedeno v následujícím grafu. Viz Graf 5.

2. Pohlaví

122 odpovědí



Graf 5 Pohlaví respondentů

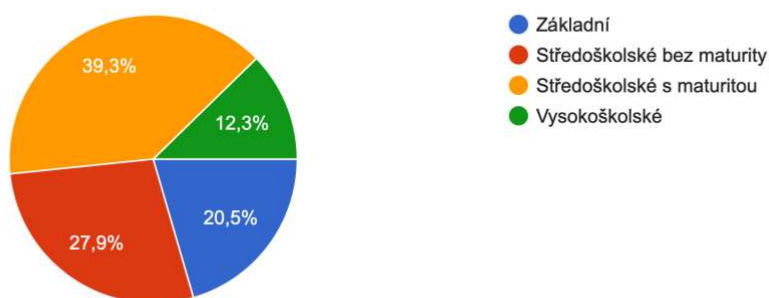
(zdroj: vlastní)

Respondenti byli v rámci třetí otázky dotázáni na svou nejvyšší úroveň vzdělání. Výsledky ukázaly, že 39,3 % respondentů má středoškolské vzdělání s maturitou, což tvoří největší skupinu. Následuje 27,9 % respondentů s dokončeným středoškolským vzděláním bez maturity, zatímco 20,5 % dotazovaných uvedlo, že jejich nejvyšší dosažené vzdělání je

základní. 12,3 % respondentů má vysokoškolské vzdělání. Tento rozptyl ukazuje na značnou diverzitu ve vzdělanosti mezi seniory, což může mít vliv na jejich schopnost orientovat se v otázkách bezpečnosti a rizik spojených s moderními technologiemi, včetně sociálního inženýrství. Vzdělání může také ovlivnit, jak respondenti rozumí a reagují na hrozby v kyberprostoru. Viz Graf 6.

3. Nejvyšší dosažené vzdělání

122 odpovědí



Graf 6 Nejvyšší dosažené vzdělání respondentů

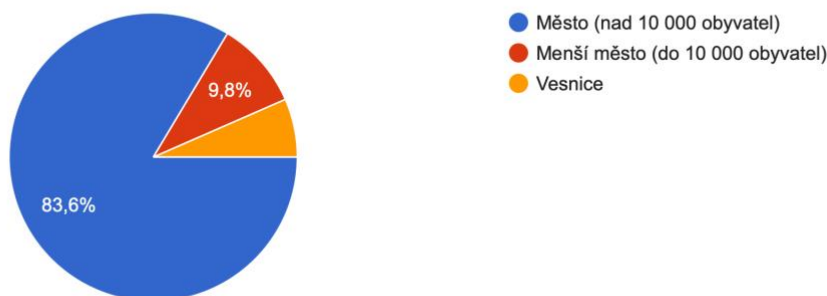
(zdroj: vlastní)

Další dvě otázky dotazníku se zaměřily na demografické údaje týkající se místa bydliště a předchozího pracovního zaměření respondentů.

Co se týče místa bydliště, výsledky ukazují, že většina respondentů žije ve městě s počtem obyvatel nad 10 000. Tento segment tvoří 83,6 % respondentů. Následuje skupina, která bydlí v menším městě do 10 000 obyvatel, což reprezentuje 9,8 % účastníků výzkumu. Nejmenší podíl, 6,6 %, tvoří respondenti žijící ve vesnici. Viz Graf 7.

4. Místo bydliště

122 odpovědí



Graf 7 Místo bydliště respondentů

(zdroj: vlastní)

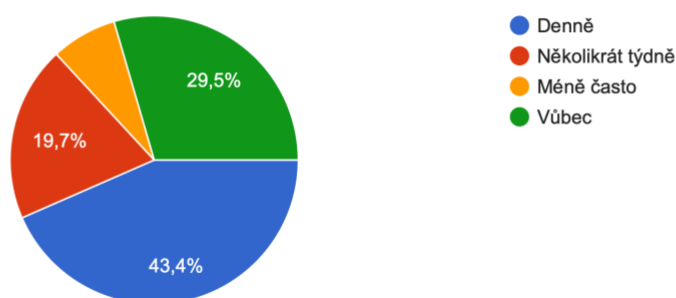
Poslední demografická otázka se zaměřila na předchozí pracovní zaměření. Největší podíl, konkrétně 32 %, respondentů se věnoval administrativní a kancelářské práci. Dalších 28,7 % respondentů pracovalo v manuálních profesích (řemeslné práce). 10,7 % se zaměřovalo na technické obory a IT, zatímco 8,2 % respondentů pracovalo ve zdravotnictví a sociální péči. Zbylých 20,4 % se věnovalo jiným oborům, které nebyly specifikovány v otázce.

6.4 Zkoumané výsledky dotazníku

V souvislosti s šestou otázkou týkající se frekvence používání internetu, bylo zjištěno, že internet je pravidelně využíván značnou částí respondentů. Konkrétně 43,4 % seniorů používá internet denně, 19,7 % několikrát týdně, 7,4 % méně často a 29,5 % ho nepoužívá vůbec. Tento výsledek poukazuje na to, že většina seniorů se pravidelně setkává s online prostředím, zatímco část seniorů je v této oblasti zcela neaktivní. Pravidelní uživatelé internetu jsou však vystaveni vyššímu riziku kybernetických hrozeb a útoků, což zdůrazňuje nutnost zvýšené pozornosti v oblasti online bezpečnosti a prevence rizik. Viz Graf 8.

6. Jak často používáte internet?

122 odpovědí



Graf 8 Frekvence používání internetu mezi respondenty

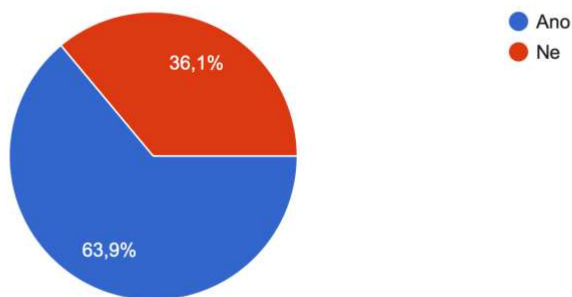
(zdroj: vlastní)

Na základě odpovědí na sedmou otázku související s používáním chytrých telefonů lze konstatovat, že 63,9 % respondentů tento typ zařízení využívá, zatímco 36,1 % uvedlo, že smartphone nevlastní. Většina seniorů používá chytré telefony, nicméně využívání těchto

zařízení může zvyšovat riziko vystavení hrozbám, které jsou spojené se sociálním inženýrstvím. U respondentů, kteří chytrý telefon nevyužívají, je pravděpodobnost vystavení těmto hrozbám nižší. Viz Graf 9.

7. Používáte smartphone (chytrý telefon)?

122 odpovědí



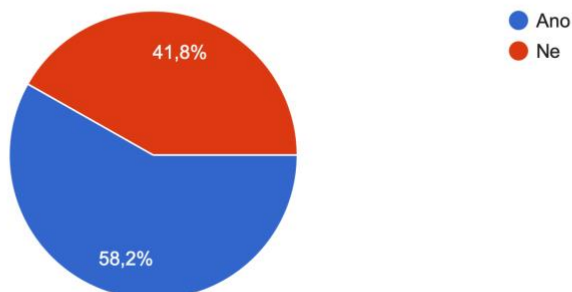
Graf 9 Používání chytrého telefonu mezi respondenty

(zdroj: vlastní)

V osmé otázce, která se týkala využívání sociálních sítí, odpovědělo 58,2 % seniorů, že je aktivně používají, zatímco 41,8 % se jim vyhýbá. Senioři využívající sociální sítě čelí výrazně vyšším rizikům spojeným se sociálním inženýrstvím. Útočníci často cílí právě na platformy jako Facebook, WhatsApp a Instagram, což zvyšuje riziko podvodných aktivit a kybernetických útoků. Viz Graf 10.

8. Používáte sociální sítě (Facebook, WhatsApp, Instagram a jiné)?

122 odpovědí



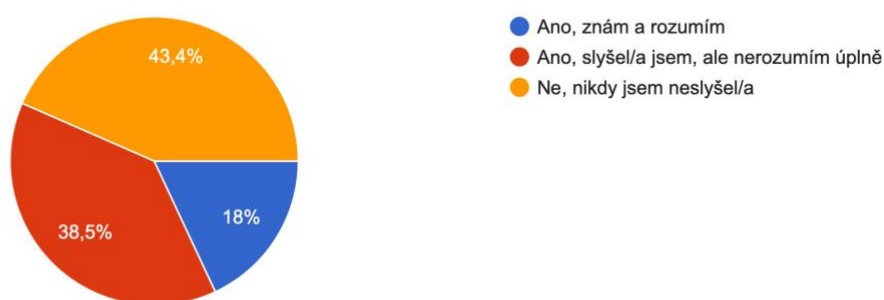
Graf 10 Používání sociálních sítí mezi respondenty

(zdroj: vlastní)

V rámci deváté otázky, která se zaměřovala na znalost pojmu „sociální inženýrství“, bylo zjištěno, že 43,4 % seniorů se s tímto termínem nikdy nesetkalo. Dalších 38,5 % respondentů mělo povědomí o tomto pojmu, avšak jeho podrobný význam jim není zcela jasný. Pouze 18 % seniorů uvedlo, že nejen znají tento pojem, ale také mu rozumí. Tento výsledek naznačuje, že povědomí o sociálním inženýrství mezi seniory je omezené. Viz Graf 11.

9. Znáte pojem „sociální inženýrství“ a víte, co znamená?

122 odpovědí



Graf 11 Znalost pojmu sociální inženýrství mezi respondenty

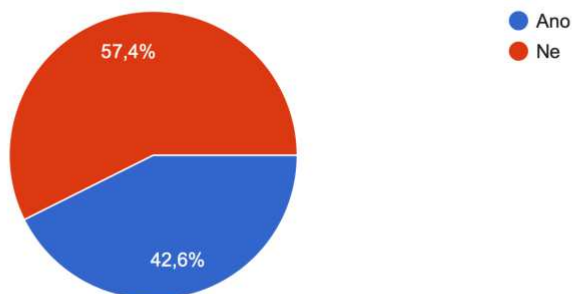
(zdroj: vlastní)

V otázkách 10, 11 a 12 se zkoumalo, zda se senioři setkali s běžnými metodami sociálního inženýrství jako je vishing, phishing a smishing.

Konkrétně v otázce 10, která se zaměřovala na vishing, uvedlo 42,6 % respondentů, že se s podvodným telefonátem, při němž byli přesvědčováni k poskytnutí citlivých informací nebo provedení finanční transakce, setkali. Oproti tomu 57,4 % seniorů tuto zkušenost nemělo. Viz Graf 12.

10. Setkali jste se někdy s podvodným telefonátem (tzv. vishing), kdy vás někdo přesvědčoval, abyste poskytli citlivé informace nebo udělali finanční transakci?

122 odpovědí



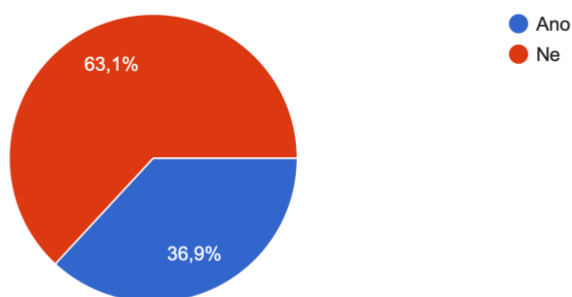
Graf 12 Setkání respondentů s vishingem

(zdroj: vlastní)

Otázka 11 se týkala phishingu, tedy podezřelých e-mailů, které vyzývají ke kliknutí na škodlivé odkazy nebo sdělení citlivých údajů. 36,9 % respondentů potvrdilo, že se s takovým e-mailem setkali, zatímco 63,1 % tuto zkušenost nemá. Viz Graf 13.

11. Setkali jste se někdy s podezřelým e-mailem, který vás nabádal ke kliknutí na odkaz nebo sdělení citlivých údajů (tzv. phishing)?

122 odpovědí



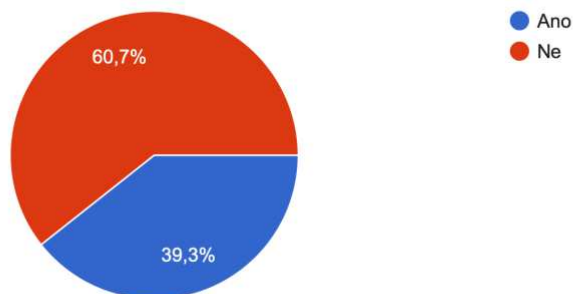
Graf 13 Setkání respondentů s phishingem

(zdroj: vlastní)

Tématem dvanácté otázky byla zkušenost respondentů s přijetím falešné SMS zprávy obsahující výzvu k akci. Z odpovědí vyplynulo, že 39,3 % seniorů již takovou zprávu obdrželo, zatímco 60,7 % respondentů se s touto formou podvodu dosud nesetkalo. Viz Graf 14.

12. Dostali jste někdy SMS zprávu, která vypadala podezřele a obsahovala výzvu k akci, například k uhrazení nedoplatku nebo kliknutí na odkaz (tzv. smishing)?

122 odpovědí



Graf 14 Setkání respondentů se smishingem

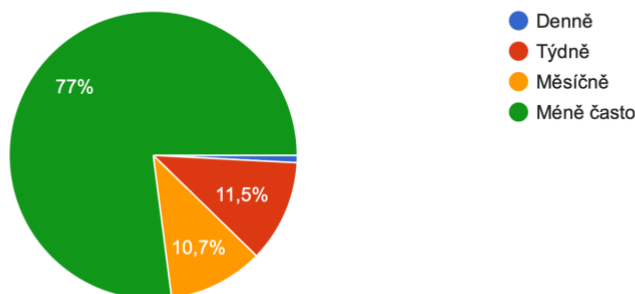
(zdroj: vlastní)

Tyto výsledky ukazují, že přestože podvody tohoto typu postihují významnou část seniorů, většina z nich se s těmito hrozbami nesetkala. Nejčastěji se senioři setkali s podvodnými telefonáty, naopak nejméně seniorů mělo zkušenost s podezřelými e-maily. Vzhledem k rostoucí sofistikovanosti těchto útoků je však důležité zaměřit se na prevenci a zvyšování povědomí seniorů o těchto typech podvodů.

Na základě výsledků třinácté otázky bylo zjištěno, že pouze 0,8 % seniorů se s podvodnými pokusy setkává denně, 11,5 % týdně, 10,7 % měsíčně a 77 % respondentů uvedlo, že se s nimi setkává méně často. Je však nezbytné upozornit na skutečnost, že si značná část osob nemusí být vědoma, že se stala terčem útoku založeného na technikách sociálního inženýrství, a to ani v případech, kdy nebyl tento útok plně realizován. Metody sociálního inženýrství jsou totiž často založeny na sofistikovaných technikách manipulace, jejichž cílem je vyvolat u oběti falešný pocit bezpečí a minimalizovat vnímání probíhajícího útoku. Viz Graf 15.

13. Jak často se setkáváte s různými typy podvodných pokusů (telefonáty, e-maily, SMS, zprávy na sociálních sítích)?

122 odpovědí



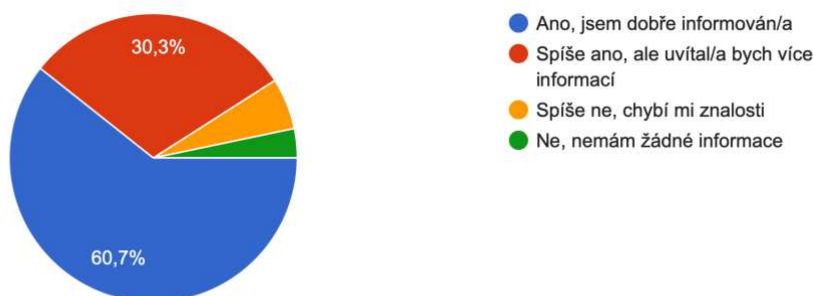
Graf 15 Frekvence setkávání se s podvodnými pokusy

(zdroj: vlastní)

Ve čtrnácté otázce uvedlo 60,7 % seniorů, že se cítí dobře informováni o způsobech rozpoznání a obrany proti podvodné komunikaci. Dalších 30,3 % respondentů uvedlo, že se sice cítí spíše informovaní, ale přivítali by více informací. Naopak 5,7 % seniorů připustilo, že jim znalosti spíše chybí, a 3,3 % respondentů uvedlo, že v této oblasti nemají žádné informace. Výsledky je však třeba interpretovat s určitou rezervou, neboť v této věkové skupině může docházet k nadhodnocování vlastních schopností. Starší lidé často vnímají své životní zkušenosti jako dostatečnou ochranu před riziky, což může vést k podcenění nových forem podvodného jednání, které využívají moderní technologie a psychologickou manipulaci. Viz Graf 16.

14. Cítíte, že máte dostatek informací o tom, jak rozpoznat podvodnou komunikaci a jak se jí bránit?

122 odpovědí



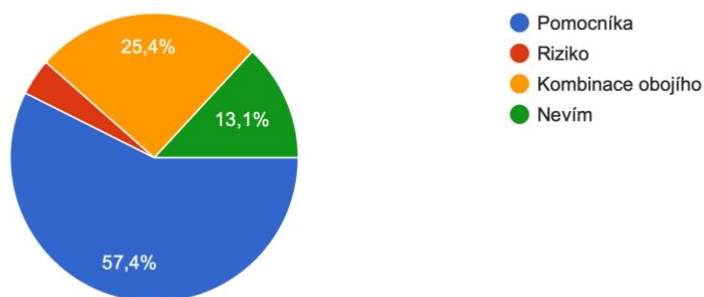
Graf 16 Schopnost respondentů rozeznat podvodnou komunikaci

(zdroj: vlastní)

Výsledky patnácté otázky ukazují, že 57,4 % respondentů vnímá internet a moderní technologie primárně jako pomocníka, 25,4 % respondentů je považuje za kombinaci pomocníka a rizika, 13,1 % respondentů uvedlo, že se nedokáže jednoznačně rozhodnout, a pouze 4,1 % dotazovaných v nich spatřuje převážně riziko. Přestože většina seniorů přistupuje k moderním technologiím s pozitivním postojem, je třeba zdůraznit, že využívání internetu vyžaduje vysokou míru ostražitosti a informovanosti. Ti, kteří internet a technologie vnímají převážně jako pomocníka, si nemusí plně uvědomovat rozmanitost hrozeb, jimž mohou čelit. Viz Graf 17.

15. Považujete internet a moderní technologie spíše za pomocníka, nebo za riziko?

122 odpovědí



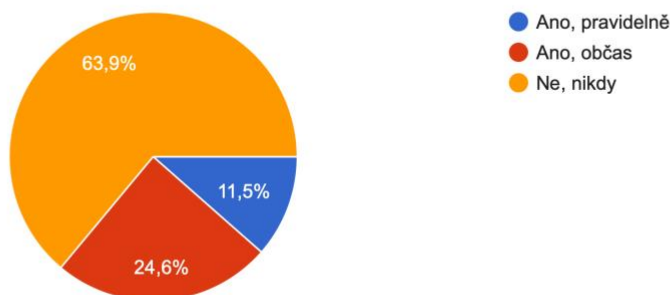
Graf 17 Vnímání internetu z pohledu respondentů

(zdroj: vlastní)

Na základě výsledků šestnácté otázky lze konstatovat, že 63,9 % seniorů uvádí, že svá hesla nebo přístupové údaje k účtům nesdělují nikomu. Přibližně čtvrtina respondentů (24,6 %) však přiznala, že tyto údaje občas sdílí, a 11,5 % tak činí pravidelně. Přestože většina seniorů chrání své přístupové údaje, skutečnost, že někteří je občas sdílí, představuje bezpečnostní riziko, protože i blízké osoby mohou nevědomky způsobit jejich zneužití. Viz Graf 18.

16. Svěřujete někomu svá hesla nebo přístupové údaje k účtům (např. rodině, známým)?

122 odpovědí



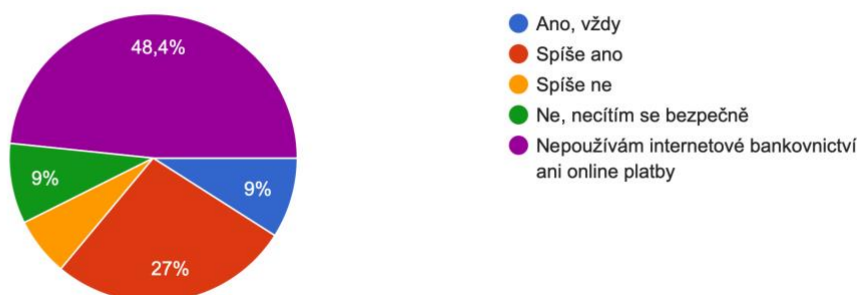
Graf 18 Svěřování hesel mezi respondenty

(zdroj: vlastní)

Z výsledků 17. otázky vyplývá, že 48,4 % seniorů nepoužívá internetové bankovníctví ani online platby, 27 % respondentů se při používání internetového bankovníctví cítí spíše bezpečně, 9 % se cítí bezpečně vždy, 9 % se necítí bezpečně a 6,6 % se spíše necítí bezpečně. Viz Graf 19.

17. Cítíte se bezpečně při používání internetového bankovníctví nebo plateb online?

122 odpovědí



Graf 19 Pocit bezpečí při používání internetového bankovníctví

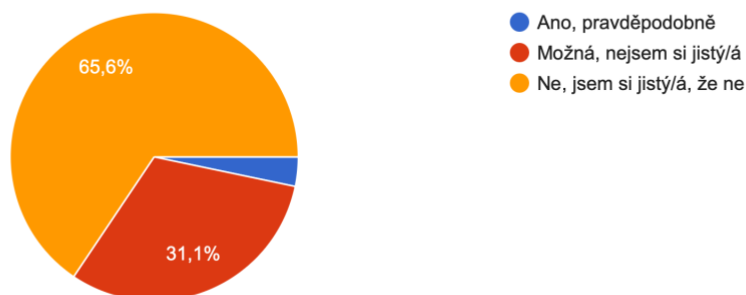
(zdroj: vlastní)

V otázce číslo 18, která se týkala přesvědčivosti podvodníků při získávání osobních nebo finančních údajů, většina respondentů, konkrétně 65,6 %, tvrdí, že by je podvodníci nemohli přesvědčit. 31,1 % si není jistých, a pouze 3,3 % se domnívá, že by je podvodníci pravděpodobně přesvědčili. Tento optimistický názor může být zkreslený přehnanou důvěrou ve vlastní schopnosti odhalit podvodnou komunikaci. Je však důležité si uvědomit,

že útoky sociálního inženýrství se stávají čím dál sofistikovanějšími a složitějšími, což znamená, že i erudovaní jednotlivci, kteří se pohybují v těchto oblastech, mohou být podvedeni. Viz Graf 20.

18. Myslíte, že by vás dokázali podvodníci přesvědčit k poskytnutí osobních nebo finančních údajů?

122 odpovědí



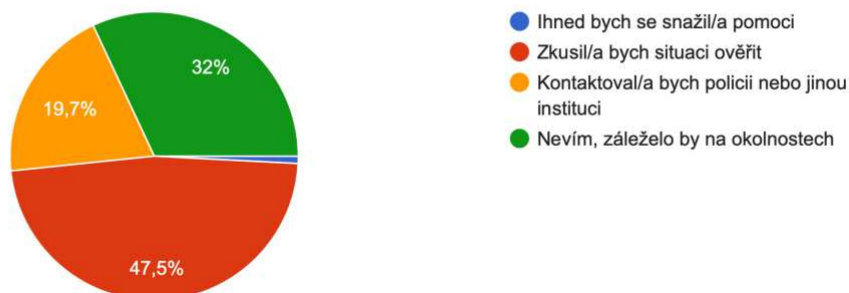
Graf 20 Přesvědčivost podvodníků podle respondentů

(zdroj: vlastní)

V devatenácté otázce se zkoumala reakce seniorů na telefonáty od osob vydávajících se za členy rodiny v nouzi, 47,5 % respondentů uvedlo, že by se pokusili situaci ověřit. 32 % si není jistých a odpovědělo, že by záleželo na okolnostech. 19,7 % by v takovém případě kontaktovalo policii nebo jinou instituci a pouze 0,8 % by okamžitě nabízelo pomoc. Tento výsledek ukazuje, že většina seniorů by se nejprve snažila ověřit pravdivost situace, což je rozumný přístup v rámci ochrany proti podvodům. Viz Graf 21.

19. Kdyby vám volal někdo, kdo se vydává za člena rodiny v nouzi, jak byste postupoval/a?

122 odpovědí



Graf 21 Reakce respondentů na telefonát od falešného rodinného příslušníka

(zdroj: vlastní)

Poslední otázka, číslo 20, byla zaměřena na zjištění názorů seniorů na opatření, která by podle nich měly instituce přijmout za účelem zlepšení ochrany před podvodným jednáním, 66,4 % respondentů uvedlo, že by uvítali zavedení lepších bezpečnostních opatření. 18 % by preferovalo větší informovanost a školení, 13,1 % by si přálo možnost jednoduššího ověření legitimacy komunikace, 1,6 % uvedlo jiné možnosti, ale nespecifikovalo je, a 0,8 % nevidí potřebu žádných změn. Tento výsledek ukazuje, že většina seniorů si uvědomuje potřebu lepších bezpečnostních opatření, ale také zdůrazňuje význam informovanosti a školení pro prevenci podvodů.

6.5 Výsledky šetření

Hlavním cílem tohoto dotazníku bylo zjištění úrovně informovanosti seniorů o sociálním inženýrství a hrozbách s ním souvisejícími. V rámci dotazníkového šetření byla na tuto otázku zaměřena zejména devátá otázka: „Znáte pojem sociální inženýrství a víte, co znamená?“ Cílem této otázky bylo ověřit nejen obeznámenost respondentů s tímto odborným termínem, ale také hloubku jejich porozumění jeho obsahu.

Výsledky ukazují, že 43,4 % dotázaných seniorů se s pojmem sociální inženýrství nikdy nesetkalo, což signalizuje poměrně nízkou míru povědomí o této problematice. Dalších 38,5 % respondentů uvedlo, že o pojmu již slyšeli, avšak jeho význam jim není zcela jasný. Pouze 18,0 % respondentů uvedlo, že nejen znají pojem sociální inženýrství, ale také rozumí jeho významu a souvislostem.

Tato zjištění svědčí o tom, že celkové povědomí o sociálním inženýrství mezi seniory je omezené. Většina dotázaných buď s tímto pojmem vůbec nepřišla do styku, nebo jej vnímá pouze povrchně, bez hlubšího porozumění jeho podstatě a skutečným hrozbám, které přináší. Vzhledem k tomu, že sociální inženýrství patří mezi často používané techniky v rámci podvodného jednání cíleného právě na seniory (např. legendy o vnucích, falešných pracovnících bank či policie), představuje tato neznalost významný faktor zvyšující jejich zranitelnost vůči těmto útokům.

6.5.1 Vyhodnocení hypotézy

Hypotéza, že senioři mají tendenci podceňovat rizika spojená s osobními údaji a věří, že je nikdo nedokáže donutit k jejich odhalení, se na základě získaných dat jeví jako potvrzená. V otázce číslo 18, která se zaměřovala na vnímanou schopnost podvodníků přesvědčit

respondenty k odhalení osobních nebo finančních údajů, uvedlo 65,6 % seniorů, že by je podvodníci pravděpodobně nepřesvědčili. Tato zjištění ukazují na výrazně optimistické vnímání vlastních schopností odolat manipulaci, které však může být zkreslené přehnanou sebedůvěrou.

Ačkoli si většina respondentů připouští jen malou pravděpodobnost, že by podlehl manipulaci, nelze přehlédnout, že útoky sociálního inženýrství jsou často natolik přesvědčivé a cílené, že mohou oklamat i zkušené a digitálně zdatné uživatele. V minulosti se oběťmi stali i lidé s technickým vzděláním nebo praxí v oboru, a to právě proto, že tyto útoky využívají momenty psychologického nátlaku, důvěry nebo časového stresu. [13]

U starší generace, která často nemá systematický přístup ke vzdělávání v oblasti kybernetické bezpečnosti, je tato důvěra potenciálně nebezpečná, jelikož může vést k nižší míře ostražitosti vůči útokům, které jsou záměrně navrženy tak, aby působily důvěryhodně a naléhavě.

V tomto světle se tedy daná hypotéza jeví jako opodstatněná. Výsledky naznačují, že značná část seniorů rizika spojená s ochranou osobních údajů podceňuje, což by mělo být důležitým impulzem pro zaměření preventivních a vzdělávacích aktivit právě na tuto oblast.

7 NÁVRH PREVENTIVNÍCH NÁSTROJŮ A POSTUPŮ PRO OCHRANU STARŠÍ GENERACE

Tato kapitola představuje konkrétní metody a postupy ochrany starší generace před útoky sociálního inženýrství, přičemž navržená opatření čerpají z teoretických poznatků a praktických znalostí získaných v práci. Pozornost je věnována praktickým preventivním opatřením, která mohou snížit zranitelnost seniorů a posílit jejich schopnost rozpoznat a odolat manipulačním technikám. Důraz je kladen na vzdělávání, osvětu a využití vhodných technických i organizačních prostředků.

7.1 Pravidelné vzdělávací semináře a školení

Jedním z účinných nástrojů pro rozpoznání sociálního inženýrství jsou pravidelné vzdělávací semináře realizované v prostředí klubů seniorů, knihoven, obecních úřadů či domovů důchodců. Tyto akce by měly mít formu interaktivních přednášek a workshopů, doplněných o simulace telefonních, SMS a e-mailových podvodů.

Hlavní náplní seminářů by bylo učení seniorů rozpoznávat rizikové situace, jako jsou například falešné telefonáty, a správně na ně reagovat. Zvláštní důraz by měl být kladen na ověřování pravosti e-mailů, SMS a zpráv na sociálních sítích a na osvojení si základních postupů při podezřelém kontaktu, a to zejména zachování klidu, neposkytování osobních údajů, okamžité ukončení komunikace a informování Policie ČR.

7.2 Edukační materiály a kampaně

Dalším z preventivních nástrojů ochrany seniorů před sociálním inženýrstvím je systematické využívání edukačních materiálů a informačních kampaní. Tyto materiály by měly být zpracovány s ohledem na specifické potřeby cílové skupiny, zejména s důrazem na srozumitelnost, jednoduchost a přehlednost.

Je vhodné vytvořit tištěné letáky a brožury, které budou obsahovat přehledná bezpečnostní doporučení a zároveň budou doplněny o konkrétní příklady nejčastějších forem podvodného jednání. Pro seniory aktivně využívající digitální technologie se navrhuje zpracování edukačních videí, krátkých podcastů a specializovaných webových stránek zaměřených na prevenci a zvýšení povědomí v oblasti kybernetické bezpečnosti.

Distribuce těchto materiálů by měla probíhat prostřednictvím míst, která senioři běžně navštěvují, například v lékárnách, na poštách, v čekárnách praktických lékařů, v rámci služby senior taxi nebo prostřednictvím terénních pečovatelských služeb.

7.3 Rodinná osvěta

Významnou roli v prevenci sociálního inženýrství sehrávají nejbližší příbuzní, kteří mohou působit jako důležitý zdroj informací a podpory. Rodinní příslušníci by měli seniory aktivně motivovat k obezřetnosti a pravidelně s nimi sdílet příklady aktuálních podvodných praktik, o nichž informují média.

Zároveň by je měli srozumitelně informovat o nových typech podvodů a v případě potřeby společně zkontrolovat nastavení soukromí na sociálních sítích, aby se minimalizovalo riziko zneužití osobních údajů.

7.4 Informování skrze média

Pro zajištění větší ochrany seniorů před podvody je důležité je pravidelně informovat prostřednictvím médií. Televize a rádio jsou vhodné kanály, jak oslovit širší veřejnost, zejména seniory. Doporučuje se vysílat krátké informační spoty mezi pořady, které jsou zaměřeny na starší generaci. Tyto spoty mohou efektivně informovat o aktuálních podvodech a poskytovat jednoduché rady, jak se jim vyhnout.

Další možností je využití tiskových médií, jako jsou časopisy. V těchto časopisech by mohly vycházet články, které seniory pravidelně upozorňují na nové podvodné praktiky a nabízejí konkrétní tipy, jak se před nimi chránit.

7.5 Technická opatření

Pro zajištění bezpečnosti digitálních zařízení je doporučeno používat antivirový software, který pomáhá chránit zařízení před malwarem a dalšími hrozbami. Kromě toho by měla být zajištěna jednoduchá a účinná ochrana účtů pomocí silných hesel a dvoufázového ověření.

Pro ochranu před nevyžádanými telefonáty je vhodné na chytrých telefonech instalovat aplikace, které blokují spam a podezřelé hovory, a také aktivovat funkce pro blokování neznámých čísel.

ZÁVĚR

V rámci této bakalářské práce je zkoumána zranitelnost starší generace vůči útokům založeným na principech sociálního inženýrství. S rostoucím zapojením seniorů do digitálního prostředí je tato skupina vystavena čím dál sofistikovanějším formám manipulace, útočníci využívají nejen technické nástroje, ale zejména lidskou důvěřivost a psychologické slabiny. V teoretické části jsou systematicky popsány klíčové pojmy, základní techniky sociálního inženýrství a faktory, které zvyšují zranitelnost jednotlivců, přičemž pozornost je věnována i technologickým prostředkům využívaným útočníky. Senioři jsou v práci identifikováni jako vysoce riziková skupina právě z důvodu nižší digitální gramotnosti, horší orientace v online prostředí a snížené schopnosti kritického vyhodnocování informací.

V praktické části jsou analyzovány konkrétní případy útoků (vishing, phishing, podvody spojené s investováním), které se v České republice v posledních letech objevují se zvyšující intenzitou. Na základě dotazníkového šetření mezi seniory byla potvrzena hlavní hypotéza práce, že senioři mají tendenci podceňovat rizika spojená s osobními údaji a věří, že je nikdo nedokáže donutit k jejich odhalení. Výsledky šetření také potvrzují, že většina respondentů má jen omezené povědomí o sociálním inženýrství a s ním spojenými hrozbami. Alarmující zůstává zejména nízká míra preventivního chování a malá schopnost identifikovat podvržené zprávy nebo neautentické webové stránky.

Na základě těchto zjištění jsou navržena konkrétní preventivní opatření zaměřená na zvyšování informovanosti seniorů – formou pravidelných školení, edukačních kampaní, rodinné osvěty, aktivní role médií a využití technických ochranných prvků. Zároveň je konstatováno, že osvěta a vzdělávání musí být přizpůsobeny schopnostem a potřebám starší generace a musejí být prezentovány přístupnou a srozumitelnou formou.

S ohledem na dynamický vývoj digitálního prostředí a postupné rozšiřování manipulativních technik se jako účelné jeví zaměřit budoucí výzkum na efektivitu jednotlivých forem prevence, možnosti personalizované edukace či vývoj nástrojů, které by seniorům aktivně a efektivně pomáhaly rozpoznat podvodné situace. Zároveň se doporučuje věnovat pozornost i mladší populaci, která často hraje klíčovou roli v předávání znalostí a budování důvěry mezi seniory a digitálním světem. Problematika sociálního inženýrství není pouze technickou výzvou, ale celospolečenským fenoménem, jehož řešení vyžaduje multidisciplinární přístup a dlouhodobou strategii.

SEZNAM POUŽITÉ LITERATURY

- [1] KOLOUCH, Jan a BAŠTA, Pavel. CyberSecurity. CZ.NIC ;. Praha : CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-34-8.
- [2] JIRÁSEK, Petr; NOVÁK, Luděk a POŽÁR, Josef. Výkladový slovník kybernetické bezpečnosti. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.
- [3] HOŘICKÝ, Martin. Metody sociálního inženýrství. Online. BDO. 2021. Dostupné z: <https://www.bdo.cz/cs-cz/temata/digital/metody-socialniho-inzenyrstvi>. [cit. 2025-05-13].
- [4] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2023. Praha: NÚKIB, 2024. Dostupné také z: <https://nukib.gov.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/>.
- [5] FOLDYNA, Tomáš. Zpráva o činnosti národního zpravodaje pro boj proti kybernetické kriminalitě, pro ochranu práv k nehmotným statkům a kybernetickou bezpečnost za rok 2023. 2024.
- [6] ŠTĚPÁNEK, Zdeněk. Inženýrství sociální. Online. Encyklopedie.soc.cas.cz. Praha: Sociologický ústav AV ČR, 2020. Dostupné z: https://encyklopedie.soc.cas.cz/w/Inzenyrstvi_socialni. [cit. 2025-05-13].
- [7] MITNICK, Kevin a SIMON, William L. The art of deception: controlling the human element of security. Indianapolis: Wiley, c2002. ISBN 978-0-7645-4280-0.
- [8] ENGEBRETSON, Patrick. The Basics of hacking and penetration Testing. Elsevier Imprint: Syngress Adresa: 225 Wyman Street, Waltham, MA 02451, USA, 2011. ISBN 978-1-59749-655-1.
- [9] Jak na kybernetickou bezpečnost: 1. díl Sociální Inženýrství. Online. Vas-hosting.cz. 2023. Dostupné z: <https://www.vas-hosting.cz/blog-jak-na-kybernetickou-bezpecnost-1-dil-socialni-inzenyrstvi>. [cit. 2025-05-13].
- [10] OZKAYA, Erdal. Learn social engineering: learn the art of human hacking with an internationally renowned expert. Birmingham: Packt, 2018. ISBN 978-1-78883-800-9. Dostupné také z: <https://ebookcentral.proquest.com/lib/natl-ebooks/detail.action?docID=5379705>.

- [11] FRUHLINGER, Josh. Social engineering: Definition, examples, and techniques. Online. Csoonline.com. 2024. Dostupné z: <https://www.csoonline.com/article/571993/social-engineering-definition-examples-and-techniques.html>. [cit. 2025-05-13].
- [12] HADNAGY, Christopher. Social engineering: the science of human hacking. Second edition. Indianapolis, IN: Wiley, [2018]. ISBN 978-1-119-43338-5.
- [13] MONTAÑEZ, Rosana; GOLOB, Edward a XU, Shouhuai. Human Cognition Through the Lens of Social Engineering Cyberattacks. Online. Frontiers in Psychology. 2020, roč. 11, s. 18. Dostupné z: <https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2020.01755/full>. [cit. 2025-05-13].
- [14] The psychology of social engineering—the “soft” side of cybercrime. Online. Microsoft.com. 2020. Dostupné z: <https://www.microsoft.com/en-us/security/blog/2020/06/30/psychology-social-engineering-soft-side-cybercrime/>. [cit. 2025-05-14].
- [15] CIALDINI, Robert B. Influence: the psychology of persuasion. EPub Edition. New York: HarperCollins, 2009. ISBN 9780061899874.
- [16] ALKHALIL, Zainab; HEWAGE, Chaminda; NAWAF, Liqaa a KHAN, Imtiaz. Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. Online. Frontiers in Computer Science. 2021, č. 3, s. 23. Dostupné z: <https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2021.563060/full>. [cit. 2025-05-13].
- [17] European Cybersecurity Month (ESCM): Tips for senior citizens. Online. National cyber security centre. 2023. Dostupné z: <https://www.ncsc.admin.ch/ncsc/en/home/aktuell/im-fokus/2023/ecsm-2023-3.html>. [cit. 2025-05-13].
- [18] REIMERS MD, Karen. Why Are Older Adults More Vulnerable to Scams? Online. Psychology today. 2023. Dostupné z: <https://www.psychologytoday.com/us/blog/the-high-cost-of-forgetting/202309/why-are-older-adults-more-vulnerable-to-scams>. [cit. 2025-05-13].

- [19] The Rise of Cybercrime Targeting Older Adults: Understanding the Threat Landscape to Prevent Attacks. Online. CSA Editorial. 2024. Dostupné z: <https://cybersecurityasia.net/rise-cyber-crime-targeting-older-adults/>. [cit. 2025-05-13].
- [20] SALAHDINE, Fatima a KAABOUC, Naima. Social Engineering Attacks: A Survey. Online. Mdpi. 2019, roč. 11, č. 4, s. 17. Dostupné z: <https://www.mdpi.com/1999-5903/11/4/89>. [cit. 2025-05-13].
- [21] INTERNET CRIME COMPLAINT CENTER. 2020 Elder Fraud Report. Washington, D.C.: Federal Bureau of Investigation, 2021. Dostupné také z: https://www.ic3.gov/AnnualReport/Reports/2020_ic3elderfraudreport.pdf.
- [22] Avoiding Social Engineering and Phishing Attacks. Online. America's Cyber Defense Agency. 2021. Dostupné z: <https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks>. [cit. 2025-05-13].
- [23] BEŠIĆ, Mustafa. Benefits and Risks of Artificial Intelligence in Cybersecurity and Phishing Attacks. Online. Big Data and Artificial Intelligence. 2023, roč. 3, č. 1, s. 5. Dostupné z: <https://ebt.rs/journals/index.php/conf-proc/article/view/175/124>. [cit. 2025-05-13].
- [24] BENZL, Lukáš. Deepfake 2024: Obranná strategie pro české firmy. Praha: Česká asociace umělé inteligence, 2023. Dostupné také z: <https://asociace.ai/wp-content/uploads/2023/12/DEEPFAKE-2024-CAUI.pdf>.
- [25] CLOUGH, Jonathan. Principles of cybercrime. Cambridge, UK: Cambridge University Press, 2010. ISBN 978-0-521-72812-6.
- [26] Malware. Online. Avast.com. Dostupné z: <https://www.avast.com/cs-cz/c-malware>. [cit. 2025-05-14].
- [27] KROMBHOLZ, Katharina; HOBEL, Heidelinde; HUBER, Markus a WEIPPL, Edgar. Advanced social engineering attacks. Online. Journal of Information Security and Applications. 2015, roč. 22, s. 10. Dostupné z: <https://www.sciencedirect.com/science/article/abs/pii/S2214212614001343>. [cit. 2025-05-14].

- [28] What is phishing? Examples, types, and techniques. Online. Csoonline.com. 2024. Dostupné z: <https://www.csoonline.com/article/514515/what-is-phishing-examples-types-and-techniques.html>. [cit. 2025-05-14].
- [29] ČESKÁ REPUBLIKA, Zákon č. 101/2000 Sb.: o ochraně osobních údajů a o změně některých zákonů. In: Sbírka zákonů. 2000. Dostupné také z: <https://www.zakonyprolidi.cz/cs/2000-101>.
- [30] EVROPSKÝ PARLAMENT a RADA EU. Nařízení Evropského parlamentu a Rady (EU) 2016/679. In: . 2016, s. 88. Dostupné také z: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32016R0679>.
- [31] 10 TYPES OF SOCIAL ENGINEERING ATTACKS AND HOW TO PREVENT THEM. Online. Crowdstrike. 2023. Dostupné z: <https://www.crowdstrike.com/en-us/cybersecurity-101/social-engineering/types-of-social-engineering-attacks/>. [cit. 2025-05-14].
- [32] Co je phishing? Online. Avast. Dostupné z: <https://www.avast.com/cs-cz/c-phishing>. [cit. 2025-05-14].
- [33] ARSHAD, Ayesha; REHMAN, Attique Ur; JAVAID, Sabeen a MUHAMMAD ALI, Tahir. A Systematic Literature Review on Phishing and Anti-Phishing Techniques. Online. Pakistan Journal of Engineering and Technology, PakJET. 2021, roč. 4, č. 1, s.6. Dostupné z: https://www.researchgate.net/publication/350512990_A_Systematic_Literature_Review_on_Phishing_and_Anti-Phishing_Techniques. [cit. 2025-05-14].
- [34] TIPTON, Harold F. a KRAUSE, Micki. Information Security Management Handbook. Sixth edition. Auerbach Publications, Taylor & Francis Group, 2008. ISBN 978-1-4200-6708-8.
- [35] JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada, 2007. ISBN 978-80-247-1561-2. Dostupné také z: <http://kramerusndk.nkp.cz/search/handle/uuid:bb517d60-f0dd-11ea-b9b3-005056827e51>.
- [36] CHAUDHURI, Ayan. Clone Phishing: Attacks and Defenses. Online. International Journal of Scientific and Research Publications. 2023, roč. 13, č. 4, s. 5. Dostupné z: <http://dx.doi.org/10.29322/IJSRP.13.04.2023.p13626>. [cit. 2025-05-14].

- [37] HODAČOVÁ, Veronika a BERÁNEK, Ladislav. Jen obezřetný senior je v bezpečí. Online. Policie České republiky. 2024. Dostupné z: https://policie.gov.cz/clanek/jen-obezretny-senior-je-v-bezpeci.aspx?utm_source=chatgpt.com. [cit. 2025-05-14].
- [38] KOVÁŘOVÁ, Anna. Od kdy je člověk senior: Jaká je věková hranice? Online. Magazín Primasenior. 2025. Dostupné z: <https://www.primasenior.cz/od-kdy-je-clovek-senior/>. [cit. 2025-05-14].
- [39] PODIVÍNSKÁ, Zuzana. Aktivizace v domovech seniorů. Bakalářská práce. Olomouc: Univerzita Palackého v Olomouci, 2014.
- [40] MARTINKOVÁ, Milada a BIEDERMANOVÁ, Eva. Senioři v České republice jako oběti i pachatelé kriminálních deliktů. Praha: Institut pro kriminologii a sociální prevenci, 2019. ISBN 978-80-7338-181-3.
- [41] Senioři v datech. Online. Český statistický úřad. 2025. Dostupné z: <https://csu.gov.cz/seniori-v-datech/vyuzivani-pc-a-internetu>. [cit. 2025-05-14].
- [42] Obezřetný senior: bezpečně v online prostředí. Praha: Policie ČR, 2024. Dostupné také z: https://budoucnostjedigitalni.gov.cz/media/material_files/brozura_Obezretny_senior_2024_na_web_j3EIhqv.pdf.
- [43] SHAO, Jingjin; ZHANG, Qianhan; REN, Yining; LI, Xiying a LIN, Tian. Why are older adults victims of fraud? Current knowledge and prospects regarding older adults vulnerability to fraud. Online. Journal of Elder Abuse & Neglect. 2019, roč. 31, č. 3. ISSN 0894-6566. Dostupné z: <https://doi.org/10.1080/08946566.2019.1625842> [cit. 2025-05-14].
- [44] SJOUWERMAN, Stu. A Generational Divide Among Social Engineering Victims. Online. KnowBe4. Dostupné z: <https://blog.knowbe4.com/a-generational-divide-among-social-engineering-victims>. [cit. 2025-05-14].
- [45] SKIBA, Katherine. Identity-Fraud Report: Older Adults Need Better Online Security. Online. AARP. 2020. Dostupné z: <https://www.aarp.org/money/scams-fraud/identity-fraud-survey-2020/>. [cit. 2025-05-14].
- [46] SENIOR proti internetovým padouchům? Online. Národní úřad pro kybernetickou a informační bezpečnost. 2022. Dostupné z: <https://osveta.nukib.gov.cz/senior>. [cit. 2025-05-14].

- [47] Na podvodném inzerátu připravil muže o 80 tisíc korun. Online. Policie České republiky. 2022. Dostupné z: <https://policie.gov.cz/clanek/na-podvodnem-inzeratu-pripravil-muze-o-80-tisic-korun.aspx>. [cit. 2025-05-14].
- [48] Další internetový podvod. Online. Policie České republiky. 2024. Dostupné z: <https://policie.gov.cz/clanek/uzemni-utvary-sprava-severoceskeho-kraje-zpravodajstvi-dalsi-internetovy-podvod.aspx>. [cit. 2025-05-14].
- [49] Další podvedený při investování. Online. Policie České republiky. 2023. Dostupné z: <https://policie.gov.cz/clanek/zpravodajstvi-z-okresu-vysetrujeme-hledame-patrame-dalsi-podvedeny-pri-investovani.aspx>. [cit. 2025-05-14].
- [50] Z televize se dozvěděl, že naletěl a hned dvakrát. Online. Policie České republiky. 2024. Dostupné z: <https://policie.gov.cz/clanek/z-televize-se-dozvedel-ze-naletel-a-hned-dvakrat.aspx>. [cit. 2025-05-14].

SEZNAM OBRÁZKŮ

Obrázek 1 Ukázka Deepfake	23
Obrázek 2 Ukázka phishingového útoku	27
Obrázek 3 Smishingový útok.....	31
Obrázek 4 Pomůcka SENIOR.....	37

SEZNAM GRAFŮ

Graf 1 Celkové počty registrovaných skutků spáchaných v kyberprostoru.....	14
Graf 2 Podíl seniorů, využívajících moderní technologie.....	33
Graf 3 Podíl seniorů, využívajících chytrý telefon	34
Graf 4 Věk respondentů	47
Graf 5 Pohlaví respondentů.....	47
Graf 6 Nejvyšší dosažené vzdělání respondentů.....	48
Graf 7 Místo bydliště respondentů.....	49
Graf 8 Frekvence používání internetu mezi respondenty	49
Graf 9 Používání chytrého telefonu mezi respondenty	50
Graf 10 Používání sociálních sítí mezi respondenty	50
Graf 11 Znalost pojmu sociální inženýrství mezi respondenty.....	51
Graf 12 Setkání respondentů s vishingem.....	52
Graf 13 Setkání respondentů s phishingem.....	52
Graf 14 Setkání respondentů se smishingem	53
Graf 15 Frekvence setkávání se s podvodnými pokusy	54
Graf 16 Schopnost respondentů rozeznat podvodnou komunikaci.....	54
Graf 17 Vnímání internetu z pohledu respondentů	55
Graf 18 Svěřování hesel mezi respondenty.....	56
Graf 19 Pocit bezpečí při používání internetového bankovníctví.....	56
Graf 20 Přesvědčivost podvodníků podle respondentů.....	57
Graf 21 Reakce respondentů na telefonát od falešného rodinného příslušníka	57

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AI	Artificial Intelligence (umělá inteligence)
ČR	Česká republika
EU	Evropská unie
EUR	Mezinárodní měnová zkratka pro euro dle ISO 4217
GDPR	General Data Protection Regulation (Obecné nařízení o ochraně osobních údajů)
IT	Information Technology (informační technologie)
Kč	Korun českých (zkratka měny České republiky)
PIN	Personal Identification Number (osobní identifikační číslo)
SMS	Short Message Service (služba krátkých textových zpráv)
USB	Universal Serial Bus (univerzální sériová sběrnice)

SEZNAM PŘÍLOH

Příloha P I: Dotazník zpracovaný v kapitole 6.

PŘÍLOHA P I: NÁZEV PRVNÍ PŘÍLOHY

Vážený respondente,

rád bych Vás požádal o vyplnění dotazníku k mé bakalářské práci na téma „Sociální inženýrství jako hrozba pro starší generace: prevence a osvěta“.

Děkuji za Váš čas a spolupráci.

Maksym Nebytov, student Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně.

Pokyny: Vyberte a zakroužkujte nejvhodnější odpověď, případně dopište vlastní.

1. Věk

☐ 60–69 let

☐ 70–79 let

☐ 80+ let

2. Pohlaví

☐ Muž

☐ Žena

☐ Jiné / nechci uvádět

3. Nejvyšší dosažené vzdělání

☐ Základní

☐ Středoškolské bez maturity

☐ Středoškolské s maturitou

☐ Vysokoškolské

4. Místo bydliště

☐ Město (nad 10 000 obyvatel)

☐ Menší město (do 10 000 obyvatel)

☐ Vesnice

5. Vaše předchozí hlavní pracovní zaměření

- ☐ Administrativa / kancelářská práce
- ☐ Technické obory / IT
- ☐ Zdravotnictví a sociální péče
- ☐ Manuální práce (řemeslné profese, výroba)
- ☐ Jiný obor (prosím uveďte) _____

6. Jak často používáte internet?

- ☐ Denně
- ☐ Několikrát týdně
- ☐ Méně často
- ☐ Vůbec

7. Používáte smartphone (chytrý telefon)?

- ☐ Ano
- ☐ Ne

8. Používáte sociální sítě? (Facebook, WhatsApp, Instagram a jiné)

- ☐ Ano
- ☐ Ne

9. Znáte pojem „sociální inženýrství“ a víte, co znamená?

- ☐ Ano, znám a rozumím
- ☐ Ano, slyšel/a jsem, ale nerozumím úplně
- ☐ Ne, nikdy jsem neslyšel/a

10. Setkali jste se někdy s podvodným telefonátem (tzv. vishing), kdy vás někdo přesvědčoval, abyste poskytli citlivé informace nebo udělali finanční transakci?

- ☐ Ano
- ☐ Ne

11. Setkali jste se někdy s podezřelým e-mailem, který vás nabádal ke kliknutí na odkaz nebo sdělení citlivých údajů (tzv. phishing)?

☐ Ano

☐ Ne

12. Dostali jste někdy SMS zprávu, která vypadala podezřele a obsahovala výzvu k akci, například k uhrazení nedoplatku nebo kliknutí na odkaz (tzv. smishing)?

☐ Ano

☐ Ne

13. Jak často se setkáváte s různými typy podvodných pokusů (telefonáty, e-maily, SMS, zprávy na sociálních sítích)?

☐ Denně

☐ Týdně

☐ Měsíčně

☐ Méně často

14. Cítíte, že máte dostatek informací o tom, jak rozpoznat podvodnou komunikaci a jak se jí bránit?

☐ Ano, jsem dobře informován/a

☐ Spíše ano, ale uvítal/a bych více informací

☐ Spíše ne, chybí mi znalosti

☐ Ne, nemám žádné informace

15. Považujete internet a moderní technologie spíše za pomocníka, nebo za riziko?

☐ Pomocníka

☐ Riziko

☐ Kombinace obojího

☐ Nevím

16. Svěřujete někomu svá hesla nebo přístupové údaje k účtům (např. rodině, známým)?

☐ Ano, pravidelně

☐ Ano, občas

☐ Ne, nikdy

17. Cítíte se bezpečně při používání internetového bankovníctví nebo plateb online?

☐ Ano, vždy

☐ Spíše ano

☐ Spíše ne

☐ Ne, necítím se bezpečně

☐ Nepoužívám internetové bankovníctví ani online platby

18. Myslíte, že by vás dokázali podvodníci přesvědčit k poskytnutí osobních nebo finančních údajů?

☐ Ano, pravděpodobně

☐ Možná, nejsem si jistý/á

☐ Ne, jsem si jistý/á, že ne

19. Kdyby vám volal někdo, kdo se vydává za člena rodiny v nouzi, jak byste postupoval/a?

☐ Ihned bych se snažil/a pomoci

☐ Zkusil/a bych situaci ověřit

☐ Kontaktoval/a bych policii nebo jinou instituci

☐ Nevím, záleželo by na okolnostech

20. Jaké kroky by podle vás měly instituce (např. banky, policie, úřady) podniknout, aby vás lépe chránily před podvody?

☐ Větší informovanost a školení

☐ Zavedení lepších bezpečnostních opatření

☐ Možnost jednoduššího ověření legitimacy komunikace

☐ Jiné (prosím specifikujte): _____